

Probity Management in Financial Regulators — Australian Prudential Regulation Authority

Australian Prudential Regulation Authority

© Commonwealth of Australia 2023

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-825-1 (Print)

ISBN 978-1-76033-826-8 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:

communication@anao.gov.au.



Canberra ACT

1 June 2023

Dear President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Australian Prudential Regulation Authority. The report is titled *Probity Management in Financial Regulators — Australian Prudential Regulation Authority*. I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — <http://www.anao.gov.au>.

Yours sincerely



Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Audit team

Grace Guilfoyle
James Sheeran
Jo Rattray-Wood
Alexandra McFadyen
Michelle Page

Contents

Summary and recommendations.....	7
Background	7
Conclusion	9
Supporting findings	9
Recommendations	11
Summary of Australian Prudential Regulation Authority response	12
Key messages from this audit for all Australian Government entities	12
Audit findings.....	13
1. Background	14
Introduction	14
The Australian Prudential Regulation Authority	22
Rationale for undertaking the audit	24
Audit approach	25
2. Arrangements to manage probity risks and promote compliance with requirements	26
Has APRA identified key probity risks and developed policies, procedures and arrangements to manage the identified risks?.....	26
Were relevant policies subject to periodic review?	57
Does APRA effectively inform its personnel of probity requirements and promote compliance?	58
3. Monitoring, reporting and assurance	61
Is there a framework for monitoring the effectiveness of internal controls relating to probity and providing assurance to the accountable authority?.....	61
Is there a framework for monitoring compliance with probity requirements, including regular monitoring and reporting?	66
Is there a framework for following up on identified instances of non-compliance?	70
4. Compliance with requirements	73
Has APRA complied with the selected probity requirements?	73
Has non-compliance been addressed in accordance with stated requirements?	87
Appendices	89
Appendix 1 Australian Prudential Regulation Authority response	90
Appendix 2 Improvements observed by the ANAO	91
Appendix 3 Department of Finance guidance — Ethics and Probity in Procurement: Principles	92



Audit snapshot

Auditor-General Report No.30 2022–23

Probity Management in Financial Regulators — Australian Prudential Regulation Authority



Why did we do this audit?

- ▶ It is essential that financial regulators uphold high probity standards, to strengthen the legitimacy and integrity of the regulator and support the objectives of the regulatory scheme.
- ▶ This is one of a series of three performance audits which continues the ANAO's examination of probity management in Commonwealth entities.
- ▶ The audit provides the Parliament with independent assurance regarding probity management at the Australian Prudential Regulation Authority (APRA).



What did we find?

- ▶ Probity management at the Australian Prudential Regulation Authority (APRA) was largely effective.
- ▶ With the exception of not having a policy for senior executive remuneration, APRA had arrangements structured to manage the probity risks selected for review, and to promote compliance.
- ▶ APRA had a framework and arrangements to monitor, report on and provide assurance on the selected probity requirements.
- ▶ APRA fully or largely complied with most of the probity related requirements examined in this audit. There was partial compliance with credit card requirements.



Key facts

- ▶ APRA is an independent statutory authority established under the *Australian Prudential Regulation Authority Act 1998*.
- ▶ APRA's purpose is to ensure Australians' financial interests are protected and the financial system is stable, competitive, and efficient.



What did we recommend?

- ▶ The Auditor-General made two recommendations aimed at: APRA establishing a policy for senior executive remuneration; and improved arrangements for the management of gifts, benefits and hospitality.
- ▶ APRA agreed to the recommendations.

844

employees at 30 June 2022.

3-5

full-time APRA Members serving on APRA's Executive Board.

1

person (the APRA Chair) is the Accountable Authority.

Summary and recommendations

Background

1. The Organisation for Economic Co-operation and Development (OECD) has observed that:
Regulation is a key tool for achieving the social, economic and environmental policy objectives of governments that cannot be effectively addressed through voluntary arrangements and other means. Governments have a broad range of regulatory powers reflecting the complex and diverse needs of their citizens, communities and economy.
Regulators are entities authorised by statute to use legal tools to achieve policy objectives, imposing obligations or burdens through functions such as licencing, permitting, accrediting, approvals, inspection and enforcement. Often they will use other complementary tools, such as information campaigns, to achieve the policy objectives, but it is the exercise of control through legal powers that makes the integrity of their decision-making processes, and thus their governance, very important.¹
2. The OECD has further observed that:
Strong governance strengthens the legitimacy and integrity of the regulator, supporting the high level policy objectives of the regulatory scheme and will lead to better outcomes.²
3. The OECD has identified two broad aspects of governance relevant to regulators:
 - external governance (looking out from the regulator) – the roles, relationships and distribution of powers and responsibilities between the legislature, the minister, the ministry, the judiciary, the regulator’s governing body and regulated entities; and
 - internal governance (looking into the regulator) – the regulator’s organisational structures, standards of behaviour and roles and responsibilities, compliance and accountability measures, oversight of business processes, financial reporting and performance management.³
4. The Australian Government’s overarching governance framework for public entities, including its regulatory agencies, is established by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the supporting Public Governance, Performance and Accountability Rule 2014 (PGPA Rule).
5. The PGPA Act contains general duties for entity accountable authorities and officials which are relevant to probity and ethics.⁴ These duties are not restricted to resource management functions, as the PGPA Act regulates entity governance, performance and accountability more broadly. The general duties establish an overarching framework for probity and ethical behaviour applying to the officials of PGPA Act entities.

1 OECD, *OECD Best Practice Principles for Regulatory Policy, The Governance of Regulators* [Internet], OECD, 2014, p. 17, available from https://read.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en#page1 [accessed 18 November 2022].

2 *ibid.*, p. 17.

3 *ibid.*, p. 19.

4 An accountable authority can be an individual or a group of individuals (such as a governing board). An accountable authority, whether an individual or a member of a governing board, is also an official under the PGPA Act and is therefore subject to the general duties of officials in sections 25 to 29 of the PGPA Act.

6. Further specific probity and ethical requirements may apply to entity personnel, including requirements established by the Parliament in the regulator's enabling legislation, other applicable laws and policy frameworks, and the internal policies and frameworks put in place by the entity's accountable authority.

Rationale for undertaking the audit

7. It is essential that financial regulators uphold high probity standards, to strengthen the legitimacy and integrity of the regulator and support the objectives of the regulatory scheme.

8. This is one of a series of three performance audits which continues the ANAO's examination of probity management in Commonwealth entities and provides independent assurance to the Parliament. It builds on Auditor-General Report No.21 2019–20 *Probity Management in Rural Research and Development Corporations*, which assessed the effectiveness of five rural research and development corporations' management of probity.

9. This series of audits focuses on probity management in entities with a role in financial regulation activities. These are the:

- Australian Competition and Consumer Commission (ACCC);
- Australian Prudential Regulation Authority (APRA); and
- Australian Securities and Investments Commission (ASIC).

Audit objective and criteria

10. The audit objective was to assess the effectiveness of APRA's probity management.

11. To form a conclusion against the objective, the ANAO adopted the following high-level criteria.

- Does APRA have arrangements structured to manage selected probity risks and promote compliance with requirements?
- Has APRA established monitoring and reporting arrangements to provide assurance on the effectiveness of internal controls and compliance with probity requirements?
- Has APRA complied with probity requirements?

12. The ANAO reviewed a selection of probity risks requiring management by Australian Government entities, including a number of specific risks requiring management by entities involved in financial regulation activities. The risks selected for review related to:

- the APRA Code of Conduct;
- the management of conflict of interest;
- the management of key regulatory risks (such as regulatory capture risk and financial trading);
- the management of senior executive remuneration;
- probity in procurement;
- the oversight of corporate credit card expenditure;
- the management of gifts, benefits and hospitality;

- the identification and management of fraud risks; and
- the management of public interest disclosures.

13. The ANAO's review focused on the period July 2020 – November 2022 and where relevant, included key subsequent events up to and including February 2023. The ANAO did not examine specific investigations into APRA personnel or review APRA's corporate governance arrangements.⁵

Conclusion

14. Probity management at the Australian Prudential Regulation Authority (APRA) was largely effective.

15. With the exception of not having a policy for senior executive remuneration, APRA has arrangements structured to manage the probity risks selected for ANAO review and arrangements to promote compliance with probity requirements.

16. APRA has a framework and arrangements for monitoring the effectiveness of internal controls and compliance with probity requirements, and for providing assurance to the accountable authority in relation to probity. The framework includes regular compliance monitoring, reporting to management and high-level governance committees, and arrangements for following up on identified instances of non-compliance. Key activities are overseen by a Risk Management and Compliance team.

17. While APRA fully or largely complied with most of the probity related requirements examined in this audit, there was partial compliance with requirements for the use of corporate credit cards.

18. There is evidence that APRA has addressed identified non-compliance with the APRA Code of Conduct, conflict of interest requirements, the disclosure of financial holdings policy, and some instances of non-compliance relating to corporate credit card use.

Supporting findings

Arrangements to manage probity risks and promote compliance with requirements

19. APRA has developed APRA Values and an APRA Code of Conduct as required by its enabling legislation. APRA has also identified key probity risks relating to: conflict of interest; financial trading; senior executive remuneration; procurement; corporate credit card expenditure; gifts, benefits and hospitality; fraud; and public interest disclosures. APRA had not explicitly identified regulatory capture risk as a risk to be managed in its entity level risk appetite statement or risk register. APRA's divisional risk register included risks that can flow from regulatory capture risk. In December 2022 APRA updated its risk register to include explicit reference to regulatory capture as one of the causes of operational risk in relation to its supervisory divisions. For the period examined in this audit, APRA had policies, procedures and arrangements to manage its

⁵ In recent years the ANAO has conducted two series of governance audits. These audits assessed the effectiveness of the governance board in public sector entities. These are available on the ANAO's website from https://www.anao.gov.au/pubs/performance-audit?query=board+governance&items_per_page=10 [accessed 3 March 2023].

identified risks, with the exception of not having a remuneration policy specifically for senior executives. (See paragraphs 2.3 to 2.120)

20. APRA has established a framework for the design and review of its policies. For the selected probity risks, there was evidence of relevant policies being reviewed and updated. (See paragraphs 2.121 to 2.123)

21. For the selected probity risks, APRA has effectively informed its personnel of probity requirements. APRA has adopted a combination of training, making information on policies, procedures and arrangements easily accessible on its intranet, and messaging from senior officials to reinforce knowledge of probity requirements and promote compliance. APRA tracks the completion of annual refresher training and reports the results to senior management. (See paragraphs 2.124 to 2.131)

Monitoring, reporting and assurance

22. APRA has a framework for monitoring the effectiveness of internal controls and providing assurance to the accountable authority in relation to probity. The framework includes regular internal audits into probity related topics and periodic assessment of control effectiveness. Reporting on internal audits and the effectiveness of internal controls is provided to the Executive Board, Executive Committee and the Audit and Risk Committee. The accountable authority is a member of the Executive Board and Executive Committee. (See paragraphs 3.3 to 3.17)

23. APRA undertakes regular compliance monitoring under its compliance management framework, and has established a Risk Management and Compliance team which reports on a regular basis to the Audit and Risk Committee and the Executive Committee on compliance with obligations, including obligations related to probity requirements. APRA's compliance management framework includes a register of compliance obligations, and Reportable Incident and Escalation Standards which establish reporting obligations. (See paragraphs 3.18 to 3.28)

24. APRA has a framework for following up on identified instances of non-compliance. The framework is documented in APRA's Compliance Management Policy, which is supported by Reportable Incident and Escalation Standards and related guidance. (See paragraphs 3.29 to 3.45)

Compliance with requirements

25. For the periods reviewed by the ANAO, APRA undertook its internal assurance processes under which relevant personnel made declarations relating to the APRA Code of Conduct and compliance with conflict of interest and financial trading requirements. Results for the respective processes were reported to senior management committees. Disclosures of APRA Members' interests were provided to the Treasurer as required under the *Australian Prudential Regulation Authority Act 1998*.

26. APRA personnel largely complied with requirements relating to gifts, benefits and hospitality. For a sample of credit card transactions reviewed, there was partial compliance with requirements relating to corporate credit card use.

27. APRA did not have a specific policy for managing senior executive remuneration, but advised that the general policy applying to staff was applied to its senior executives in practice. At a high level, the process APRA adopted for senior executive remuneration was consistent with the general staff remuneration policy. There is evidence that the APRA Chair was provided with

information on, and approved, individual remuneration outcomes for all members of the senior executive cohort for the most recent review process that involved a pay rise.

28. APRA's procurement policies and guidance require officials to comply with the Commonwealth Procurement Rules (CPRs). APRA's procurement policies and guidance do not outline any further specific requirements for the management of probity related risks. For the ten high-value procurements reviewed by the ANAO, APRA documented the requirement to consider probity as part of the procurement process in seven cases. Two of the 10 procurements examined were incorrectly reported on AusTender and for one procurement, the evaluation criteria limited competition contrary to the requirements of the CPRs.

29. There is scope for APRA to enhance its requirements in relation to gifts, benefits and hospitality. (See paragraphs 4.3 to 4.52)

30. There is evidence that identified instances of non-compliance were addressed by APRA in accordance with its requirements for: breaches of the financial holdings disclosure policy; annual code of conduct declaration process; and annual declaration of conflicts of interest process.

31. There is evidence of some instances of non-compliance identified by APRA, or in the context of this audit, being addressed in accordance with APRA's requirements in relation to corporate credit card use.

32. There is no evidence of instances of non-compliance identified by APRA, or in the context of this audit, being addressed in accordance with APRA's requirements for: procurement; and gifts, benefits and hospitality. (See paragraphs 4.53 to 4.60)

Recommendations

Recommendation no. 1 The Australian Prudential Regulation Authority develop and issue a remuneration policy for its senior executives.
Paragraph 2.53

Australian Prudential Regulation Authority response: *Agreed.*

Recommendation no. 2 The Australian Prudential Regulation Authority strengthen its gifts, benefits and hospitality arrangements by:
Paragraph 4.49

- (a) requiring the recipients of offers of gifts, benefits and hospitality to record in the internal register whether accepting the offer represents a real or perceived conflict of interest and document the basis for their decision to accept; and
- (b) reviewing whether its policy settings adequately support the established internal principle of officials generally seeking to avoid the receipt of gifts and offers of hospitality.

Australian Prudential Regulation Authority response: *Agreed.*

Summary of Australian Prudential Regulation Authority response

33. The proposed audit report was provided to APRA. APRA provided the summary response below. The full response from APRA is provided at Appendix 1. The improvements observed by the ANAO during the course of this audit are at Appendix 2.

The Australian Prudential Regulation Authority (APRA) welcomes the ANAO's report on Probity Management in Financial Regulators. APRA is committed to continuous improvement in Probity Management and accepts the recommendations contained in the ANAO's report, to enable the organisation to continue to uphold high probity standards.

Key messages from this audit for all Australian Government entities

34. This audit is one of a series of probity management audits that apply a standard methodology to probity management in financial regulators. The three entities included in the ANAO's 2022–23 probity management in financial regulators series are the:

- Australian Competition and Consumer Commission (ACCC);
- Australian Prudential Regulation Authority (APRA); and
- Australian Securities and Investments Commission (ASIC).

35. Key messages from the ANAO's series of probity management audits will be outlined in an upcoming Audit Insights product available on the ANAO website.

Audit findings

1. Background

Introduction

Government regulators

1.1 The Organisation for Economic Co-operation and Development (OECD) has observed that:

Regulation is a key tool for achieving the social, economic and environmental policy objectives of governments that cannot be effectively addressed through voluntary arrangements and other means. Governments have a broad range of regulatory powers reflecting the complex and diverse needs of their citizens, communities and economy.

Regulators are entities authorised by statute to use legal tools to achieve policy objectives, imposing obligations or burdens through functions such as licencing, permitting, accrediting, approvals, inspection and enforcement. Often they will use other complementary tools, such as information campaigns, to achieve the policy objectives, but it is the exercise of control through legal powers that makes the integrity of their decision-making processes, and thus their governance, very important.⁶

Regulator governance

1.2 The OECD has further observed that:

Strong governance strengthens the legitimacy and integrity of the regulator, supporting the high level policy objectives of the regulatory scheme and will lead to better outcomes.⁷

1.3 The OECD has identified two broad aspects of governance relevant to regulators:

- external governance (looking out from the regulator) – the roles, relationships and distribution of powers and responsibilities between the legislature, the minister, the ministry, the judiciary, the regulator’s governing body and regulated entities; and
- internal governance (looking into the regulator) – the regulator’s organisational structures, standards of behaviour and roles and responsibilities, compliance and accountability measures, oversight of business processes, financial reporting and performance management.⁸

6 OECD, *OECD Best Practice Principles for Regulatory Policy, The Governance of Regulators* [Internet], OECD, 2014, p. 17, available from https://read.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en#page1 [accessed 18 November 2022].

Professor Malcolm K. Sparrow similarly observed in 2000 that: ‘The important features that distinguish regulatory and enforcement agencies from the rest of government are precisely the important features that they share. The core of their mission involves the imposition of duties. They deliver obligations, rather than services. ...Their routine use of state authority and coercion distinguishes them from the rest of government and carries its own distinct strategic and managerial challenges.’ Sparrow, M. K., *The Regulatory Craft*, Brookings Institution Press, Washington DC, 2000, p. 2.

7 OECD, *OECD Best Practice Principles for Regulatory Policy, The Governance of Regulators* [Internet], OECD, 2014, p. 17, available from https://read.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en#page1 [accessed 18 November 2022].

8 *ibid.*, p. 19.

1.4 The OECD has described these components of external and internal governance as the ‘different building blocks that make up the governance architecture of regulators’.⁹

Duties of Australian Government officials

1.5 The Australian Government’s overarching governance framework for public entities, including its regulatory agencies, is established by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the supporting Public Governance, Performance and Accountability Rule 2014 (PGPA Rule).

1.6 The PGPA Act contains general duties for entity accountable authorities and officials which are relevant to probity and ethics.¹⁰ These duties are not restricted to resource management functions, as the objects of the PGPA Act (and its overview section) make clear that the Act is concerned with entity governance, performance and accountability more broadly (see Box 1 below).

Box 1: Objects and overview of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act)

Objects of the PGPA Act (section 5)

The objects of this Act are:

- (a) to establish a coherent system of governance and accountability across Commonwealth entities; and
- (b) to establish a performance framework across Commonwealth entities; and
- (c) to require the Commonwealth and Commonwealth entities:
 - (i) to meet high standards of governance, performance and accountability; and
 - (ii) to provide meaningful information to the Parliament and the public; and
 - (iii) to use and manage public resources properly; and
 - (iv) to work cooperatively with others to achieve common objectives, where practicable; and
- (d) to require Commonwealth companies to meet high standards of governance, performance and accountability.

Overview of the PGPA Act (section 6)

This Act is mainly about the governance, performance and accountability of Commonwealth entities.

9 OECD, *The Governance of Regulators, Governance of Regulators' Practices: Accountability, Transparency and Co-ordination* [Internet], OECD, 2016, p. 16, available from https://read.oecd-ilibrary.org/governance/governance-of-regulators-practices_9789264255388-en#page1 [accessed 18 November 2022].

10 An accountable authority can be an individual or a group of individuals (such as a governing board). An accountable authority, whether an individual or a member of a governing board, is also an official under the PGPA Act and is therefore subject to the general duties of officials in sections 25 to 29 of the PGPA Act.

Box 1: Objects and overview of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act)

It is also about:

- the use and management of public resources by the Commonwealth and Commonwealth entities; and
- the accountability of Commonwealth companies.

1.7 The requirements of the PGPA Act and PGPA Rule, including the general duties of entity officials, may extend to persons who are not entity employees (such as contractors) if they are considered to be entity officials under the Act. Contract provisions may also extend PGPA Act and PGPA Rule requirements (and elements of the *Public Service Act 1999* (PS Act), discussed below) to persons who are not entity employees.¹¹

1.8 As at 6 March 2023 there were 189 PGPA Act entities and companies.¹² The duties of entity accountable authorities and officials under the PGPA Act are summarised in Box 2 below.

Box 2: General duties of accountable authorities and officials

General duties of accountable authorities (extracts)

Section 15 — Duty to govern the Commonwealth entity

(1) The accountable authority of a Commonwealth entity must govern the entity in a way that:

- (a) promotes the proper use and management of public resources for which the authority is responsible; and
- (b) promotes the achievement of the purposes of the entity; and
- (c) promotes the financial sustainability of the entity.

11 Auditor-General Report No.43 2021–22 *Effectiveness of the Management of Contractors — Department of Defence*, pp. 16–22.

This was one of a series of three performance audits — in the Department of Defence, the Department of Veterans' Affairs and Services Australia — which examined the management of contractors by Australian Public Service (APS) agencies. Chapter 5 of this audit report set out high-level observations and key messages for all APS agencies, including in respect to the application of ethical and personnel security requirements to the contractor workforce. The ANAO observed in paragraphs 5.4–5.5 that individual agencies determine the extent to which the ethical and integrity frameworks that apply to APS employees (which include the ethical requirements of the PS Act and the PGPA Act) also apply to contractors and other non-APS personnel engaged by the agency. These decisions are captured in, and managed through, contracts. This discretionary approach applies in an agency operating environment where a large number of contractors are doing work in and as part of the operations of APS agencies, alongside APS personnel, as part of a mixed workforce. On that basis, the rationale for a discretionary approach is not clear. One risk of adopting a discretionary approach is that it may give rise to unequal behavioural expectations across personnel types within workplaces, and the risk of inconsistent management of personnel behaviours.

12 The PGPA Act Flipchart and List published by the Department of Finance (Finance) provides a summary of all non-corporate and corporate Commonwealth entities and companies. These resources are available from <https://www.finance.gov.au/government/managing-commonwealth-resources/structure-australian-government-public-sector/pgpa-act-flipchart-and-list> [accessed 6 April 2023].

Box 2: General duties of accountable authorities and officials

Note: Section 21 (which is about the application of government policy) affects how this duty applies to accountable authorities of non-corporate Commonwealth entities.

(2) In making decisions for the purposes of subsection (1), the accountable authority must take into account the effect of those decisions on public resources generally.

General duties of officials (extracts)***Section 25 — Duty of care and diligence***

(1) An official of a Commonwealth entity must exercise his or her powers, perform his or her functions and discharge his or her duties with the degree of care and diligence that a reasonable person would exercise if the person:

- (a) were an official of a Commonwealth entity in the Commonwealth entity's circumstances; and
- (b) occupied the position held by, and had the same responsibilities within the Commonwealth entity as, the official.

(2) The rules may prescribe circumstances in which the requirements of subsection (1) are taken to be met.

Section 26 — Duty to act honestly, in good faith and for a proper purpose

An official of a Commonwealth entity must exercise his or her powers, perform his or her functions and discharge his or her duties honestly, in good faith and for a proper purpose.

Section 27 — Duty in relation to use of position

An official of a Commonwealth entity must not improperly use his or her position:

- (a) to gain, or seek to gain, a benefit or an advantage for himself or herself or any other person; or
- (b) to cause, or seek to cause, detriment to the entity, the Commonwealth or any other person.

Section 28 — Duty in relation to use of information

A person who obtains information because they are an official of a Commonwealth entity must not improperly use the information:

- (a) to gain, or seek to gain, a benefit or an advantage for himself or herself or any other person; or
- (b) to cause, or seek to cause, detriment to the Commonwealth entity, the Commonwealth or any other person.

Section 29 — Duty to disclose interests

(1) An official of a Commonwealth entity who has a material personal interest that relates to the affairs of the entity must disclose details of the interest.

Box 2: General duties of accountable authorities and officials

(2) The rules may do the following:

- (a) prescribe circumstances in which subsection (1) does not apply;
- (b) prescribe how and when an interest must be disclosed;
- (c) prescribe the consequences of disclosing an interest (for example, that the official must not participate at a meeting about a matter or vote on the matter).

Probity

1.9 Taken together, the general duties establish an overarching framework for probity and ethical behaviour applying to the officials of PGPA Act entities.

1.10 The Australian Government Department of Finance (Finance), which administers the PGPA Act and PGPA Rule and is the framework policy owner, has not included a general definition of probity in its PGPA Glossary.¹³ Finance has, however, adopted the following definition of probity in the procurement context:

Probity is the evidence of ethical behaviour, and can be defined as complete and confirmed integrity, uprightness and honesty in a particular process.¹⁴

1.11 While intended to inform those involved in procurement activity, this definition of probity is sufficiently robust to describe the general expectation applying to Australian Government activity more broadly, including regulatory activity.

1.12 The specific probity and ethical requirements applying to the personnel of an Australian Government entity will depend on what type of entity it is, the legislation applying to it, the government policies and frameworks applying to it, and the internal policies and frameworks it has put in place. In summary.

- Whether the entity is a non-corporate Commonwealth entity or a corporate Commonwealth entity¹⁵ under the PGPA Act, will determine which elements of the framework established by the PGPA Act and PGPA Rule will apply to the entity. In particular, entity type will affect whether certain activity-specific frameworks apply to an entity.

13 Department of Finance, *PGPA Glossary* [Internet], available from <https://www.finance.gov.au/about-us/glossary/pgpa/term-ethical> [accessed 23 May 2023].

The glossary includes the following definition of ethical:

(in relation to the proper use of public resources) The extent to which the proposed use is consistent with the core beliefs and values of society. Where a person behaves in an ethical manner it could be expected that a person in a similar situation would undertake a similar course of action. For the approval of proposed commitments of relevant money, an ethical use of resources involves managing conflicts of interests, and approving the commitment based on the facts without being influenced by personal bias. Ethical considerations must be balanced with whether the use will also be efficient, effective and economical. [emphasis in original]

14 Department of Finance, *Ethics and Probity in Procurement: Principles* [Internet], 17 May 2021, available from <https://www.finance.gov.au/government/procurement/buying-australian-government/ethics-and-probity-procurement> [accessed 9 February 2023].

15 Corporate Commonwealth entities are legally separate from the Commonwealth. The Finance Flipchart recorded that there were 100 non-corporate Commonwealth entities and 72 corporate Commonwealth entities as at 6 March 2023.

- Activity-specific frameworks can establish ethical and probity requirements specific to the activity they regulate, and cover grants administration¹⁶, government procurement¹⁷, government advertising¹⁸, protective security¹⁹, appearing before the

16 Department of Finance, *Commonwealth Grants Rules and Guidelines 2017* [Internet], Finance, available from <https://www.finance.gov.au/government/commonwealth-grants/commonwealth-grants-rules-and-guidelines> [accessed 21 November 2022].

The Australian Government grants policy framework applies to all non-corporate Commonwealth entities subject to the PGPA Act.

17 Department of Finance, *Commonwealth Procurement Rules* [Internet], Finance, 1 July 2022, available from <https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules> [accessed 21 November 2022].

Officials from non-corporate Commonwealth entities and prescribed corporate Commonwealth entities listed in section 30 of the PGPA Rule must comply with the Commonwealth Procurement Rules when performing duties related to procurement.

18 Department of Finance, *Australian Government Guidelines on Information and Advertising Campaigns by non-corporate Commonwealth entities* [Internet]. Interim Guidelines were in effect from July 2022, available from <https://www.finance.gov.au/government/advertising/australian-government-guidelines-information-and-advertising-campaigns-non-corporate-commonwealth-entities> [accessed 21 November 2022].

Non-corporate Commonwealth entities under the PGPA Act must comply with the Guidelines.

19 Attorney-General's Department, *Protective Security Policy Framework (PSPF)* [Internet], AGD, available from <https://www.protectivesecurity.gov.au/> [accessed 21 November 2022].

The PSPF applies to non-corporate Commonwealth entities subject to the PGPA Act to the extent consistent with legislation. The PSPF represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies under the PGPA Act. Non-government organisations that access security classified information may be required to enter into a deed or agreement to apply relevant parts of the PSPF for that information.

Parliament²⁰, liaising with lobbyists²¹, caretaker conventions²², risk management²³ and fraud control.²⁴ These frameworks will generally specify which types of entities they cover and may also place specific obligations on the accountable authority, such as to promote an internal culture supportive of the purposes of the framework.²⁵

- Entities established under legislation are statutory bodies and will also be subject to the requirements of that legislation. The entity's enabling legislation may include specific ethical

20 Department of the Prime Minister and Cabinet, *Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters – February 2015* [Internet], PM&C, available from <https://www.pmc.gov.au/resource-centre/government/government-guidelines-official-witnesses-parliamentary-committees-and-related-matters-february-2015> [accessed 21 November 2022].

The guidelines state that they are 'designed to assist departmental and agency officials, statutory office holders and the staff of statutory authorities in their dealings with the parliament. The term 'official' is used throughout the *Guidelines*; it includes all persons employed by the Commonwealth who are undertaking duties within a Commonwealth department or agency (whether employed under the PS Act or other legislation) and those in government business enterprises, corporations and companies. It is recognised, however, that the role and nature of some statutory office holders and their staff will require the selective application of these *Guidelines*, depending on the individual office holder's particular statutory functions and responsibilities.'

21 Attorney-General's Department, *Australian Government Register of Lobbyists and Lobbying Code of Conduct* [Internet], AGD, available from <https://www.ag.gov.au/integrity/australian-government-register-lobbyists> [accessed 21 November 2022].

Under the code, Australian Government representatives must only meet with third-party lobbyists who are registered. Under the code Australian Government representatives include an agency head or a person employed under the PS Act, a person engaged as a contractor or consultant by an Australian Government agency whose staff are employed under the PS Act, and a member of the Australian Defence Force.

22 Department of the Prime Minister and Cabinet, *Guidance on Caretaker Conventions 2021* [Internet], PM&C, available from <https://www.pmc.gov.au/resource-centre/government/guidance-caretaker-conventions> [accessed 21 November 2022].

The guidance states that: 'The conventions and practices have developed primarily in the context of the relationship between ministers and their departments (and executive agencies since the commencement of the PS Act). The relationship between ministers and other Australian Government entities and bodies, such as statutory authorities and government companies, varies depending on the specific body. All bodies should observe the conventions and practices, unless doing so would conflict with their legal obligations or compelling organisational requirements.'

23 Department of Finance, *Commonwealth Risk Management Policy* [Internet], Finance, 1 January 2023, available from <https://www.finance.gov.au/about-us/news/2022/revised-commonwealth-risk-management-policy-2023> [accessed 1 February 2023].

The Policy was developed to support section 16 of the PGPA Act, which requires accountable authorities to maintain systems of risk oversight, management and internal control. The Policy is mandatory for all non-corporate Commonwealth entities and recommended as best practice for corporate Commonwealth entities.

24 Attorney-General's Department, *Commonwealth Fraud Control Framework* [Internet], AGD, available from <https://www.counterfraud.gov.au/library/commonwealth-fraud-control-framework> [accessed 21 November 2022].

The Framework comprises three tiered documents — the fraud rule, fraud policy and fraud guidance — with different binding effects for corporate and non-corporate Commonwealth entities. Non-corporate Commonwealth entities must comply with the fraud rule and fraud policy. The fraud guidance is not binding, however the government considers the guidance to be better practice and expects entities to follow it where appropriate.

25 For example, Element Three of the 2023 *Commonwealth Risk Management Policy* states that 'Culture is shaped by the behaviours and attitudes of leaders. The desired culture for managing risk should be clearly defined and demonstrated by the executive in a form that is communicated and actively promoted to staff. An entity's internal policies should also be aligned to its desired culture.' The fraud guidance under the Commonwealth Fraud Control Framework states that accountable authorities play a key role in setting the ethical tone within their entities, and fostering and maintaining a culture of fraud awareness and prevention.

- obligations applying to the accountable authority and/or entity staff. Individual statutory offices are also established through legislation, which may include ethical requirements.
- Other applicable legislation may place further ethical and probity requirements on the entity. Examples include anti-corruption legislation²⁶ and corporations law requirements. As at 6 March 2023, there were 17 Commonwealth controlled companies subject to the *Corporations Act 2001*.
 - If the entity is subject to the PS Act²⁷, additional ethical and probity requirements apply to Australian Public Service (APS) employees, including the APS Values and APS Code of Conduct.²⁸
 - Section 10 of the PS Act sets out the APS Values. Subsection 10(2), ‘Ethical’, states that ‘The APS demonstrates leadership, is trustworthy, and acts with integrity, in all that it does.’ The APS Commissioner’s Directions (31 January 2022) made under the PS Act elaborate on the APS Values. Section 14 of the Directions sets out requirements to be met to uphold the ‘Ethical’ value, ‘having regard to an individual’s duties and responsibilities’. The requirements include: ‘acting in a way that models and promotes the highest standard of ethical behaviour’, ‘complying with all relevant laws, appropriate professional standards and the APS Code of Conduct’ and ‘acting in a way that is right and proper, as well as technically and legally correct or preferable’. Section 12 of the PS Act provides that an APS Agency Head ‘must uphold and promote the APS Values and APS Employment Principles’.
 - Australian Public Service Commission (APSC) guidance highlights that integrity covers several different and overlapping aspects that relate to conduct and how APS employees work individually and collectively. Integrity includes: compliance with

26 Established under the *Law Enforcement Integrity Commissioner Act 2006* (LEIC Act), the Australian Commission for Law Enforcement Integrity (ACLEI) oversees the integrity of Australian Government law enforcement agencies and selected regulators. The Integrity Commissioner investigates allegations of corruption involving current or former staff members of the Australian Competition and Consumer Commission (ACCC); Australian Prudential Regulation Authority (APRA); and Australian Securities and Investments Commission (ASIC).

Australian Commission for Law Enforcement Integrity, *About the Commission* [Internet], available from <https://www.aclei.gov.au/about-aclei/about-commission> [accessed 23 November 2022].

In November 2022 the Australian Parliament passed legislation to establish a new National Anti-Corruption Commission (NACC), with jurisdiction over the Commonwealth public sector as a whole. ACLEI will be subsumed into the NACC. The NACC is expected to begin operations in mid-2023.

On 9 December 2022 ACLEI launched a Commonwealth Integrity Maturity Framework to assist Commonwealth entities to assess and plan to improve their integrity systems in preparation for the commencement of the NACC.

Australian Commission for Law Enforcement Integrity, *Commonwealth Integrity Maturity Framework* [Internet], available from <https://www.aclei.gov.au/preventing-corruption/commonwealth-integrity-maturity-framework> [accessed 1 February 2023].

27 The Australian Public Service Commission (APSC) reported that in 2020–21, 97 Australian Government entities employed staff under the PS Act.

Australian Public Service Commission, *State of the Service Report 2020-21* [Internet], APSC, available from <https://www.apsc.gov.au/initiatives-and-programs/workforce-information/research-analysis-and-publications/state-service/state-service-report-2020-21/appendix-2-aps-agencies> [accessed 18 November 2022].

28 Australian Public Service Commission, *APS Values and Code of Conduct in practice* [Internet], APSC, 13 September 2021, available from <https://www.apsc.gov.au/publication/aps-values-and-code-conduct-practice> [accessed 18 November 2022].

legislative frameworks, policies and practices, and ensures standards for integrity are being met; a values-based approach that promotes ethical decision-making; institutional integrity, where organisational systems, policies and practices are purposeful, legitimate and trustworthy; and a pro-integrity culture, in which there is a positive, conscious effort to make integrity a central consideration of all activities.²⁹

- A number of specific probity requirements apply to APS Senior Executive Service (SES) employees and/or APS agency heads.³⁰ These include the declaration of interests³¹ and the declaration of gifts, benefits and hospitality.³²
- Entity-specific frameworks include an entity's internal policies and guidance in respect of implementing applicable laws and frameworks. Examples include Accountable Authority Instructions (AAIs) made under the PGPA Act³³, and internal integrity frameworks. Entity-specific frameworks may sometimes establish higher expectations than the minimum standards established by whole-of-government policy owners such as Finance. Professional codes and standards may also apply to entity personnel working in certain sectors or roles. The need for such codes and standards may be specified in legislation applying to the entity.

The accountable authority's role in promoting probity

1.13 As discussed in paragraph 1.6, the PGPA Act places a number of duties on an entity's accountable authority. As discussed in paragraph 1.12, other applicable frameworks will also place obligations on entity leaders, such as the promotion of an appropriate culture. The ANAO has previously observed that in order to fulfil its governing role in relation to probity, the accountable authority would be expected to set out roles and reporting within the entity, approve and review probity policies, ensure it is informed about the entity's activities, act on information promptly, and take an active role when working with management.³⁴

The Australian Prudential Regulation Authority

1.14 The Australian Prudential Regulation Authority (APRA) is an independent statutory authority. It was established under and administers the *Australian Prudential Regulation Authority Act 1998* (APRA Act). APRA's *Corporate Plan 2022–23* states that 'APRA is the financial sector's

29 Australian Public Service Commission, *Fact sheet: Defining Integrity* [Internet], APSC, 9 December 2021, available from <https://www.apsc.gov.au/node/1532> [accessed 20 November 2022].

30 Australian Public Service Commission, *Integrity in the APS* [Internet], APSC, 8 December 2021, available from <https://www.apsc.gov.au/working-aps/integrity> [accessed 20 November 2022].

31 Australian Public Service Commission, *Declaration of interests* [Internet], APSC, 7 March 2019, available from <https://www.apsc.gov.au/working-aps/integrity/integrity-resources/declaration-interests> [accessed 20 November 2022].

32 Australian Public Service Commission, *Guidance for Agency Heads—Gifts and Benefits* [Internet], APSC, available from <https://www.apsc.gov.au/working-aps/integrity/integrity-resources/guidance-agency-heads-gifts-and-benefits> [accessed 20 November 2022].

33 AAIs are written instruments that may be issued by the accountable authority to instruct officials on matters relating to the PGPA Act framework. AAIs assist accountable authorities in meeting their general duties under the PGPA Act and establishing appropriate internal controls for their entity. Finance guidance on AAIs is available from <https://www.finance.gov.au/government/managing-commonwealth-resources/managing-risk-internal-accountability/duties/risk-internal-controls/accountable-authority-instructions-aais-rmg-206> [accessed 18 November 2022].

34 Auditor-General Report No.21 2019–20 *Probity Management in Rural Research and Development Corporations*, p. 17.

prudential supervisor. Its purpose is to ensure Australians' financial interests are protected and the financial system is stable, competitive, and efficient.³⁵ APRA's *Annual Report 2021–22* states that 'APRA currently supervises financial institutions holding \$8.6 trillion in assets for Australian depositors, policyholders and superannuation fund members.'³⁶

1.15 APRA is a non-corporate Commonwealth entity for the purposes of the PGPA Act. It is one of three entities that have body corporate status but are prescribed in their enabling legislation as non-corporate Commonwealth entities.³⁷ Unlike most non-corporate Commonwealth entities, APRA does not engage employees under the PS Act but instead engages employees under section 45 of the APRA Act.

1.16 APRA is comprised of Members who are appointed by the Governor-General on the advice of the Australian Government.³⁸ The APRA Chair³⁹ is the accountable authority of APRA and is responsible for determining the APRA Values and the APRA Code of Conduct under sections 48AB and 48AC of the APRA Act respectively.

Oversight arrangements

1.17 APRA is subject to a range of oversight arrangements. These include the following.

- The Australian Commission for Law Enforcement Integrity (ACLEI).⁴⁰ APRA came under ACLEI's jurisdiction on 1 January 2021.⁴¹

35 Australian Prudential Regulation Authority, *Corporate Plan 2022–23* [Internet], APRA, p. 4, available from <https://www.apra.gov.au/sites/default/files/2022-08/APRA%20Corporate%20Plan%202022-23.pdf> [accessed 26 November 2022].

36 Australian Prudential Regulation Authority, *Annual Report 2021–22* [Internet], APRA, p. 8, available from https://www.apra.gov.au/sites/default/files/2022-10/APRA%202021-22%20Annual%20Report_2.pdf [accessed 26 November 2022].

37 APRA was established as a body corporate under section 13(1) of the APRA Act. However, pursuant to section 13(2) of the APRA Act, APRA is taken to be a non-corporate Commonwealth entity for the purposes of the Commonwealth finance law. Section 8 of the PGPA Act provides that 'finance law' means the PGPA Act, or the rules made under section 101 of the PGPA Act, or any instrument made under the PGPA Act, or an Appropriation Act.

38 Under the APRA Act, there are at least three, but no more than five, full-time APRA Members. As per section 1.3 of APRA's Executive Board Charter, when the APRA Members meet formally, they meet as the Executive Board.

39 The APRA Act provides for the appointment of an APRA Chair and up to two Deputy Chairs. APRA refers to these roles as Chair and Deputy Chair respectively.

40 ACLEI provides oversight in relation to the integrity of Australian Government law enforcement agencies. According to its website, ACLEI's key activities are to:

- detect corruption and enhance ACLEI partner agencies' capability to detect corruption;
- receive and assess notifications and referrals of alleged corrupt conduct by members of law enforcement agencies;
- conduct investigations into serious and systemic corrupt conduct;
- support partner law enforcement agencies to conduct their own investigations; and
- prevent corruption through engagement, support and identification of vulnerabilities.

Australian Commission for Law Enforcement Integrity, *About the Commission* [Internet], ACLEI, available from <https://www.aclei.gov.au/about-aclei/about-commission> [accessed 21 November 2022].

41 Other Australian Government entities subject to ACLEI's jurisdiction include: the Australian Competition and Consumer Commission; Australian Criminal Intelligence Commission; Australian Federal Police; Australian Securities and Investments Commission; Australian Taxation Office; Australian Transaction Reports and Analysis Centre; Department of Agriculture, Water and the Environment; and Department of Home Affairs (including the Australian Border Force).

- The Financial Regulator Assessment Authority (FRAA). The FRAA was established in 2021 in response to recommendations of the 2019 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the Hayne Royal Commission).⁴² The FRAA's role is to assess and report on the effectiveness and capability of APRA and the Australian Securities and Investments Commission (ASIC).⁴³

1.18 In addition, the House of Representatives Standing Committee on Economics has undertaken inquiries into APRA and its operations⁴⁴, including implementation of recommendations from the APRA Capability Review undertaken in response to a recommendation of the Hayne Royal Commission.

Rationale for undertaking the audit

1.19 It is essential that financial regulators uphold high probity standards, to strengthen the legitimacy and integrity of the regulator and support the objectives of the regulatory scheme.

1.20 This is one of a series of three performance audits which continues the ANAO's examination of probity management in Commonwealth entities and provides independent assurance to the Parliament. It builds on Auditor-General Report No.21 2019–20 *Probity Management in Rural Research and Development Corporations*, which assessed the effectiveness of five rural research and development corporations' management of probity.

1.21 This series of audits focuses on probity management in entities with a role in financial regulation activities. These are the:

- Australian Competition and Consumer Commission (ACCC);
- Australian Prudential Regulation Authority (APRA); and
- Australian Securities and Investments Commission (ASIC).

42 K M Hayne, *Final Report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* [Internet], available from <https://www.royalcommission.gov.au/banking> [accessed 11 April 2023].

43 The FRAA undertakes an assessment of aspects of each agency's effectiveness and capability every two years. The FRAA completed its first report on ASIC in August 2022, which assessed: strategic prioritisation, planning and decision-making; surveillance; and licensing.

Financial Regulator Assessment Authority, *Effectiveness and Capability Reviews of the Australian Securities and Investments Commission* [Internet], FRAA, July 2022, available from <https://fraa.gov.au/sites/fraa.gov.au/files/2022-08/asic-assessment-report.pdf> [accessed 21 October 2022].

During this ANAO audit, in December 2022, the FRAA commenced the consultation stage of its review on the effectiveness and capability of APRA, examining its supervision and resolution functions, focusing on superannuation.

Financial Regulator Assessment Authority, *Effectiveness and capability review of the Australian Prudential Regulation Authority* [Internet], available from <https://fraa.gov.au/consultations/effectiveness-and-capability-review-australian-prudential-regulation-authority>.

44 See for example, reports of the House of Representatives Standing Committee on Economics relating to:

- *Review of the Australian Prudential Regulation Authority Annual Report 2019 (Second Report)* [Internet], Parliament of Australia, 9 December 2020, available from https://www.aph.gov.au/Parliamentary_Business/Committees/House/Economics/APRAAnnualReport2019-2/Report [accessed 27 March 2023].
- *Review of the Australian Prudential Regulation Authority Annual Report 2019* [Internet], Parliament of Australia, 2 March 2020, available from https://www.aph.gov.au/Parliamentary_Business/Committees/House/Economics/APRAREview2018/Report [accessed 27 March 2023].

Audit approach

Audit objective, criteria and scope

1.22 The audit objective was to assess the effectiveness of APRA's probity management.

1.23 To form a conclusion against the objective, the ANAO adopted the following high level criteria.

- Does APRA have arrangements structured to manage selected probity risks and promote compliance with requirements?
- Has APRA established monitoring and reporting arrangements to provide assurance on the effectiveness of internal controls and compliance with probity requirements?
- Has APRA complied with probity requirements?

1.24 The audit scope was the period July 2020 – November 2022 and where relevant, included key subsequent events up to and including February 2023. The ANAO did not examine specific investigations into APRA personnel or review APRA's corporate governance arrangements.⁴⁵

Probity risks examined in this audit

1.25 The ANAO reviewed a selection of probity risks requiring management by Australian Government entities, including a number of specific risks requiring management by entities involved in financial regulation activities. The risks selected for review related to:

- the APRA Code of Conduct;
- the management of conflict of interest;
- the management of key regulatory risks (such as regulatory capture risk and financial trading);
- the management of senior executive remuneration;
- probity in procurement;
- the oversight of corporate credit card expenditure;
- the management of gifts, benefits and hospitality;
- the identification and management of fraud risks; and
- the management of public interest disclosures.

Audit methodology

1.26 The audit methodology included reviewing entity documentation and meeting with entity personnel.

1.27 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately \$389,000.

1.28 The team members for this audit were Grace Guilfoyle, James Sheeran, Jo Rattray-Wood, Alexandra McFadyen and Michelle Page.

45 In recent years the ANAO has conducted two series of governance audits. These audits assessed the effectiveness of the governance board in public sector entities. These are available on the ANAO's website from https://www.anao.gov.au/pubs/performance-audit?query=board+governance&items_per_page=10 [accessed 3 March 2023].

2. Arrangements to manage probity risks and promote compliance with requirements

Areas examined

This chapter examines whether the Australian Prudential Regulation Authority (APRA) has arrangements structured to manage selected probity risks and promote compliance with requirements. The selected risks relate to: code of conduct, conflict of interest; key regulatory functions; senior executive remuneration; procurement; corporate credit card expenditure; gifts, benefits and hospitality; fraud; and public interest disclosures. The period examined in this audit was July 2020 – November 2022 and where relevant, key subsequent events up to and including February 2023.

Conclusion

With the exception of not having a policy for senior executive remuneration, APRA has arrangements structured to manage the probity risks selected for ANAO review and arrangements to promote compliance with probity requirements.

Areas for improvement

The ANAO made one recommendation relating to establishing a policy for senior executive remuneration.

The ANAO also identified two opportunities for improvement in relation to: the inclusion of references to regulatory capture risk and its management in APRA's corporate plan; and improving consistency in the identification and management of probity risks in procurement.

2.1 An entity's accountable authority and management are responsible for establishing and promoting a culture of ethical behaviour within the entity. Identifying key probity risks and establishing, maintaining and promoting policies, procedures and arrangements to manage those risks helps ensure probity risks are being effectively managed in accordance with relevant requirements and consistent with community expectations.

2.2 This chapter examines whether APRA has:

- identified key probity risks and developed policies, procedures and arrangements to manage the identified risks;
- ensured policies and procedures are maintained; and
- effectively informed relevant people of probity related requirements, to promote compliance.

Has APRA identified key probity risks and developed policies, procedures and arrangements to manage the identified risks?

APRA has developed APRA Values and an APRA Code of Conduct as required by its enabling legislation. APRA has also identified key probity risks relating to: conflict of interest; financial trading; senior executive remuneration; procurement; corporate credit card expenditure; gifts, benefits and hospitality; fraud; and public interest disclosures. APRA had not explicitly identified regulatory capture risk as a risk to be managed in its entity level risk appetite

statement or risk register. APRA's divisional risk register included risks that can flow from regulatory capture risk. In December 2022 APRA updated its risk register to include explicit reference to regulatory capture as one of the causes of operational risk in relation to its supervisory divisions. For the period examined in this audit, APRA had policies, procedures and arrangements to manage its identified risks, with the exception of not having a remuneration policy specifically for senior executives.

APRA Values and Code of Conduct

2.3 The APRA Chair has established APRA Values⁴⁶ and an APRA Code of Conduct as required by the *Australian Prudential Regulation Authority Act 1998* (APRA Act).⁴⁷ The APRA Values and Code of Conduct are available on APRA's intranet site.⁴⁸

2.4 The APRA Code of Conduct states that:

This Code applies to you if you:

Are an employee of APRA or occupy a position (whether as a contractor, consultant or otherwise within APRA) and are:

- in APRA's workplace; or
- conducting business on behalf of APRA from an external location; or
- participating in work-related functions or events; or
- outside of work where your conduct may impact in any way on APRA's reputation, your colleagues, APRA employees or APRA business; or
- have access to APRA's information and communication technology systems.⁴⁹

2.5 The APRA Code of Conduct sets out the standards of behaviour APRA expects from employees or contractors providing goods or services to APRA. It states that:

The Code of Conduct, alongside APRA's Values, outlines how we expect you to carry out any activities where you represent APRA ...

You should demonstrate the highest standards of professional conduct and integrity at all times by living the APRA Values and upholding this Code, as well as the obligations and responsibilities imposed by other APRA policies ...

APRA staff should act to the highest ethical standards at all times and in all of their dealings.

...

46 The APRA Values are integrity, collaboration, accountability, respect and excellence.

47 Section 48AB of the APRA Act states that: 'The Chair must determine, in writing, the APRA Values' and 'The Chair must uphold and promote the APRA Values.' Section 48AC states that: 'The Chair must determine, in writing, the APRA Code of Conduct.'

48 During the audit fieldwork (March to November 2022) the code of conduct on APRA's external website was the version with an approval date of 21 November 2017 rather than the same version that was on APRA's intranet dated December 2020. APRA advised the ANAO in January 2023 that this was an oversight. APRA updated the code of conduct on its website on 2 February 2023.

49 Section 48AC of the APRA Act states that the APRA Code of Conduct applies to APRA Members and staff appointed under section 45 of the APRA Act.

If you breach the standards of conduct set out in the Code, you may face disciplinary action up to, and including, termination of employment.

2.6 The code identifies expectations in a range of areas, including

- in relation to personal, professional and ethical behaviour;
- reporting suspected violations of the code;
- investigating potential code violations; and
- awareness of the code.

2.7 APRA also has a Professional and Ethical Behaviour Policy⁵⁰ which ‘applies to all employees regarding any professional or social activity related to APRA such as entity interactions, work events or social media representations.’ This policy states that:

Employee behaviour should be consistent with the Code of Conduct, APRA Values and this policy, and includes:

- refraining from engaging in, assisting or encouraging any unlawful behaviour that has the potential to impact their employment; and
- reporting any unacceptable behaviour as set out in this policy.

2.8 It further states that ‘APRA employees should act to the highest ethical standards at all times and in all of their dealings.’

2.9 APRA’s risk appetite statement (December 2022) states that:

APRA has no appetite in its employees not adhering to the organisation’s frameworks, policies and procedures, including the Code of Conduct.

...

The delivery of APRA’s purpose involves the handling of sensitive and confidential information. This information relates to the industries and entities it regulates as well as the domestic and international agencies it interacts with. Further, APRA also is responsible for safeguarding sensitive and personal information relating to its employees. As such, APRA **accepts a very low tolerance** for material instances of inappropriate disclosure of confidential/sensitive information in the course of performing its activities. [emphasis in original]

Conflict of interest

2.10 APRA has identified conflict of interest as a key probity risk and developed policies, procedures and arrangements to manage the identified risks.

2.11 APRA has identified activities, actions and decisions that compromise its independence, as a risk to its effectiveness. For example, APRA’s divisional risk register has identified the following risk related to conflict of interest for APRA’s Risk Management and Compliance team:

Conflicts arise due to lack of fit for purpose conflicts framework.

50 The purpose of the policy is: ‘To promote a safe and inclusive workplace by setting the standard of professional and ethical behaviour consistent with APRA’s Code of Conduct and Values.’

There is a risk that APRA's Risk Management and Compliance team RM&C fails to develop and appropriately administer a fit for purpose Conflicts of Interest Framework which could lead to APRA not being able to effectively deliver on its mandate.

2.12 In addition, three of APRA's business units (Insurance, Banking and Superannuation) have identified in their divisional risk registers the following risk related to conflict of interest:

There is a risk that APRA's approach to managing and monitoring actual, perceived or potential conflicts involving supervisors is inadequate and/or ineffective which could lead to operational, reputational and prudential impacts, including (but not limited to): fraud, insider trading, negative media attention and external scrutiny, and other adverse outcomes for APRA.

2.13 As referenced in Box 2 in Chapter 1 of this audit, section 29 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) establishes a duty to disclose interests and requires officials of Commonwealth entities who have a material personal interest that relates to the affairs of the entity to disclose the details of the interest. The APRA Act also establishes requirements around disclosure and the management of conflicts of interest.⁵¹ In the section on 'Ethical behaviour' the APRA Code of Conduct states that:

You are also expected to:

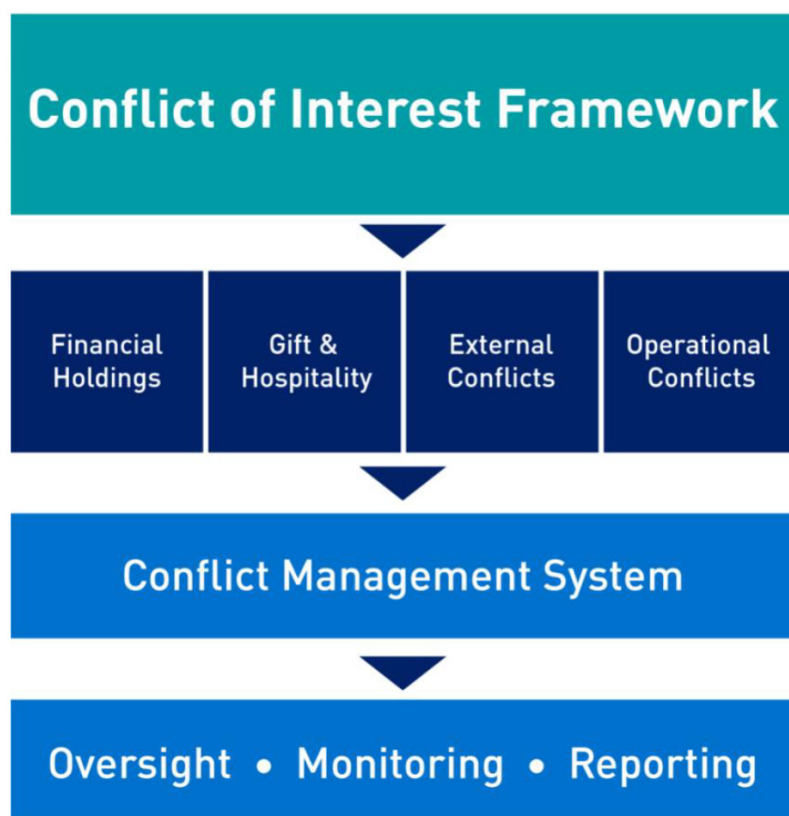
...

- avoid any conflict of interest (real or perceived) in connection with your employment, including disclosing internal or external personal relationships that may be perceived as a conflict of interest;
- immediately advise your line management where other employment or business activities (including paid or unpaid activities) create a conflict of interest (real or perceived) with the interests of APRA;
- take reasonable steps to avoid accepting gifts, benefits, offers of hospitality, compensation or consideration that might reasonably be expected to create a conflict of interest, and promptly report any gifts and benefits received and given; ...

2.14 To support the management of risks related to conflict of interest, APRA has developed a Conflicts of Interest Framework (the Framework) which states that: 'This framework establishes the conflicts management arrangements fundamental to the integrity of APRA's independent regulatory decision-making and supervisory processes.' The Framework includes procedures and processes for different types of conflicts, which are outlined in the Conflicts of Interest Procedure. Figure 2.1 illustrates the Conflicts of Interest Framework.

51 Part 4A of the APRA Act establishes responsibilities for APRA Members to disclose certain interests to the Minister and to each of the other APRA Members. Section 48D requires 'The Chair to ensure adequate disclosure of interests requirements apply to APRA staff members and delegates.'

Figure 2.1: APRA Conflicts of Interest Framework



Source: APRA Conflicts of Interest Framework June 2022.

2.15 The Framework applies to:

any person acting on behalf of APRA, including APRA Members, full and part-time employees of APRA, contractors⁵², secondees or any other individual with access to APRA's systems and records. For ease of reference, all of the above are referred to as 'employees' for the purposes of the Framework.

2.16 The Framework states that APRA:

is committed to identifying, declaring and managing conflicts of interest (conflicts). Conflicts need to be managed properly to avoid actual or perceived improper influence over APRA's decision-making. Acting under the influence of a conflict of interest may have significant consequences for APRA and the specific individual employee. This could include legal action and reputation damage.

APRA's Conflicts of Interest Framework (the Framework) outlines the arrangements to manage actual or perceived conflicts, ensuring that APRA's integrity as an effective regulator is, to the extent possible, not compromised and our employees uphold the highest standards of behaviour.

52 The Framework defines contractors as those 'who have privileged access (i.e. administrative rights to APRA systems or databases) or access to APRA's systems and records, specifically information protected under the APRA Act or the Privacy Act.'

2.17 The Framework also states that it:

is designed to ensure, amongst other things, that APRA adheres to its statutory obligations under the APRA Act, including:

- s48AC – APRA Code of Conduct;
- s48A and 48B – disclosure of interest obligations of APRA Members; and
- s48D – disclosure of interest requirements applying to APRA staff members and delegates.

2.18 The Framework defines conflict of interest⁵³ and describes four categories of conflicts covered by the Framework. These are:

- financial holdings/interests⁵⁴;
- gifts and hospitality⁵⁵;
- operational conflicts⁵⁶; and
- external conflicts.⁵⁷

2.19 The Framework also outlines, among other things:

- roles and responsibilities in relation to the management of conflicts;
- when and how conflicts are to be disclosed or reported; and

53 The Framework states that: 'A conflict of interest refers to a situation where an individual – or group of individuals – may derive or be perceived to derive a direct or indirect personal benefit (financial or otherwise) from decisions made in their official capacity, or to have a personal interest in their outcome.'

54 Probity risks related to financial holdings/interests are discussed in paragraphs 2.37 to 2.45.

55 Probity risks related to gifts and hospitality are discussed in paragraphs 2.97 to 2.103.

56 The Framework states that: 'Conflicts may arise within the context of normal operational APRA activities' and outlines 'a non-exhaustive list of potential operational conflict scenarios.' These include situations where potential conflicts could arise, such as: procurement; pecuniary interests; non-pecuniary interests; prior employment; personal or family relationships between APRA employees; personal or family relationships with third parties; non-rotation of staff and entities APRA supervises; and confidential information.

57 For example, external directorships and additional employment outside APRA.

- procedures, processes and management strategies for managing different types of conflicts.⁵⁸

2.20 APRA has also established a number of controls that stem from the Framework. For example, ‘APRA Members, and employees are required to complete a conflicts of interest declaration within one (1) month of commencing employment with APRA, and thereafter annually.’ The Framework states that:

APRA Members and employees are required to submit an annual declaration of conflicts of interest:

- that they have read and understood this policy and that they have complied with the policy over the course of the preceding year;
- that they have declared any direct security holdings in APRA-regulated entities (or close associates of regulated institutions), and those of their immediate family, family trust or self-managed superannuation fund;
- that they confirm any changes to the existing holdings;
- in the event that any financial holdings are managed by a Financial Advisor, they have provided written instruction to their Financial Advisor not to invest in APRA regulated entities;
- that they have declared any material relationship/s or arrangement/s with APRA-regulated entities, or entities that may be related to or associates of APRA-regulated entities, that are not a commercial arm’s-length arrangement; and
- that they have declared any arrangement or relationship that may create, or be perceived to create, conflicts of interest.

2.21 The Framework states that:

Annual declarations are reviewed by Risk Management & Compliance and a report is prepared and provided to the senior executive of APRA.⁵⁹ If there are any issues identified, further

58 The Conflicts of Interest Procedure outlines three main mechanisms that should be used to deal with actual or perceived conflicts of interest. These are:

- Assessing and disclosing conflicts, noting that ‘materiality should be considered having regard to the possible impact of the conflict’.
- Controlling conflicts, for example through: segregation of duties; internal structures; information barriers; and internal protocols for managing confidential information. Practical examples of strategies include:
 - system access removed from specific information systems;
 - visibility of all correspondence or decisions by line manager/General Manager/Executive Director;
 - employee recusing themselves from participating in certain activities related to the situation (i.e. attending meetings, interviews, correspondence, decisions);
 - employee being removed from involvement; and
 - employee moving roles in the team or Division.
- Avoiding conflicts, where a conflict has ‘such a serious impact, or potentially serious impact on APRA that the only way to manage them is to avoid them entirely by removing the source of the conflict.’

Management strategies are also provided for examples of potential conflicts, such as: employees with financial holdings; employees who have relationships with a key decision maker at an APRA regulated entity; or employees with conflicts relating to prior or secondary employment.

59 APRA advised the ANAO in March 2023 that this refers to APRA’s Executive Committee.

clarification or information may be sort [sic] from the employee as part of the review process. APRA may request an updated declaration at any time.

2.22 Under the Framework:

If an employee identifies an actual, potential or perceived conflict, regardless of whether the employee is involved in the conflict directly, the employee must immediately report it to his/her manager, RM&C [Risk Management and Compliance] or P&C [People and Culture] as necessary and if, the conflict is material, record the matter in APRA's conflict management system ...

2.23 APRA Members have specific obligations to make their conflict of interest disclosure to the Minister in writing, in addition to each of the other APRA Members 'as soon as practicable after the Member becomes aware of the actual or perceived conflict of interest.'⁶⁰

2.24 The Professional and Ethical Behaviour Policy discussed in paragraph 2.7 contains a section regarding conflicts of interest that includes a statement on the need to adhere to the Framework.

2.25 Internal compliance with APRA's conflict of interest declaration requirements is discussed in Chapter 4 of this audit in paragraphs 4.8 to 4.12.

Key entity-wide risks relating to regulatory activities

2.26 The ANAO examined whether APRA had identified regulatory capture risk and other key risks relating to its regulatory activities and established policies, procedures and arrangements to effectively manage those risks. The audit scope focused on entity-wide policies, procedures and arrangements and not those that only applied to certain specific roles or activities.

2.27 At the time of conducting audit fieldwork (March 2022 – November 2022) APRA had not explicitly identified regulatory capture risk as a risk to be managed in its entity level risk appetite statement or risk register. Risks that may flow from regulatory capture were included in APRA's risk register. APRA had also identified risks relating to its officials trading in financial instruments and

60 The Framework states that:

APRA Members have a standing obligation to disclose any actual or perceived conflict of interest that could conflict with the proper performance of the functions of their office. Disclosure is required whether or not there is any specific matter under consideration that gives rise to an actual or perceived conflict of interest.

The disclosure must be by notice in writing given to the Minister, and to each of the other APRA Members, as soon as practicable after the Member becomes aware of the potential or actual conflict of interest. Such conflicts will also need to be reported to the next Executive Board meeting.

At a minimum, a declaration of conflicts must be a standing item on each Executive Board agenda and relevant Committee agenda, and declaration of conflicts of interest is required to be included in the Terms of References for each Committee. Any conflicts declared at the respective meetings will be documented in the minutes of those meetings. At the discretion of the relevant Chair, employees who are identified as having a conflict may be required to abstain from participating in the meeting for the relevant item including being excluded from any discussion or decision on the matter or, if the matter is deferred or adjourned to a later date, any subsequent discussion or decision. The employee should also be excluded from any discussion on the matter leading up to the presentation to Executive Board or the relevant Committee. As per normal meeting protocols, any abstention will be recorded in the meeting.

information security.⁶¹ APRA has established policies, procedures and arrangements to manage these risks.

Regulatory capture risk

2.28 Maintaining independence is crucial for regulators to effectively perform their function. The 2019 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the Hayne Royal Commission) stated that ‘the risk of regulatory capture is well acknowledged’.⁶² The Parliamentary Joint Committee on Corporations and Financial Services, in its 2019 report on *Statutory Oversight of the Australian Securities and Investments Commission, the Takeovers Panel and the Corporations Legislation*, stated that:

The committee considers that regulatory capture is a significant issue faced by Australian regulators generally, given the size and power of corporations that operate in Australia.⁶³

2.29 The committee defined regulatory capture as:

instances where regulators are excessively influenced or effectively controlled by the industry they are supposed to be regulating. There are three areas in which particular risks arise for regulatory capture:

- staff moving between industry and regulatory jobs;
- secondments; and
- where regulatory staff are embedded in private sector organisations (that is, required to conduct their work within the workplace of industry participants, away from their home base at the regulator).⁶⁴

2.30 The need to maintain independence is reflected in APRA’s 2018 Statement of Expectations and Statement of Intent.⁶⁵ No mention is made in either regarding the risk of regulatory capture. The Statement of Expectations also states that:

In its annual Corporate Plan, APRA should identify any relevant risks and opportunities that may affect its ability to achieve its mission, and articulate clearly how its strategic priorities address and reflect these risks and opportunities.

61 The ANAO’s review of information security focussed on high level review of APRA’s risk documentation and monitoring and reporting arrangements.

62 K M Hayne, *Final Report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* [Internet], p. 443, available from <https://www.royalcommission.gov.au/banking> [accessed 11 April 2023].

63 Joint Committee on Corporations and Financial Services, *Statutory Oversight of the Australian Securities and Investments Commission, the Takeovers Panel and the Corporations Legislation*, Report No. 1 of the 45th Parliament, February 2019, p. 54, paragraph 3.49, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Corporations_and_Financial_Services/No1of45thParliament/Report [accessed 30 October 2022].

64 *ibid.*, p. 31, paragraph 3.24.

65 Sometimes entities are provided with a Statement of Expectations from their Minister. These statements generally outline the Minister’s key priorities and set out the Government’s expectations for the entity, including the priorities it is expected to observe in conducting its operations. Entities then respond to their Minister as to how they intend to deliver the identified priorities through a Statement of Intent.

The Statement of Expectations 2018 (the most recent) is available on APRA’s website from <https://www.apra.gov.au/statement-of-expectations-2018> [accessed 22 March 2023].

The Statement of Intent – September 2018 (the most recent) is available on APRA’s website from <https://www.apra.gov.au/statement-of-intent-september-2018> [accessed 22 March 2023].

2.31 The Public Governance, Performance and Accountability Rule 2014 (PGPA Rule)⁶⁶ sets out requirements entities have to comply with in relation to their corporate plans. This includes that corporate plans include ‘a summary of the risk oversight and management systems of the entity, and the key risks that the entity will manage and how those risks will be managed’.⁶⁷ APRA’s Corporate Plan 2022–23 provides a description of APRA’s key risks but does not reference the risk of regulatory capture. It includes references to APRA values, including integrity. As noted in paragraphs 2.3 to 2.6, APRA’s Code of Conduct sets out the standards of behaviour expected of APRA employees and contractors. This includes behaving honestly and with integrity in connection with employment.

2.32 At the time of conducting audit fieldwork (March 2022 – November 2022) APRA had not explicitly identified regulatory capture risk as a risk to be managed in its entity level risk appetite statement or risk register. APRA’s divisional risk register included risks that can flow from regulatory capture risk. These include bribery and corruption risk⁶⁸, data fraud risk⁶⁹ and supervisory fraud risk.⁷⁰ In December 2022 APRA updated its risk register to include explicit reference to regulatory capture as one of the causes of operational risk in relation to its supervision divisions of Banking, Insurance, and Superannuation.⁷¹

66 The PGPA Act is supported by the PGPA Rule. The PGPA Rule prescribes a range of matters that are necessary or convenient to be prescribed for the purposes of carrying out or giving effect to the PGPA Act. Sections 16E and 27A of the PGPA Rule set out the matters that the accountable authority must include in the entity’s corporate plan.

67 See section 16E of the PGPA Rule.

PGPA Rule 2014 [Internet], available from <https://www.legislation.gov.au/Details/F2022C01102> [accessed 9 March 2023].

68 APRA’s risk register identified: ‘Bribery & Corruption Risk – Bribery or corruption by APRA staff or an external party causes financial loss or reputational damage. Examples include misuse of position, manipulation of recruitment or promotion processes, accepting bribes to award contracts, accepting kickbacks, collusion, conflicts of interest, etc.’

69 APRA’s risk register identified: ‘Data Fraud Risk – Deliberate misuse or manipulation of data to provide to an unauthorised party or for personal gain, also includes bribery and corruption. Includes entity information, Policy documentation, Approvals, Licensing Applications and other APRA data. Manipulation of an entit[y’s] licensing application for personal gain, to create a gain for the entity, to cause a loss to APRA or impact APRA’s reputation. APRA employee manipulates policy documentation or an approval for personal gain or to provide a gain or cause a loss to a regulated entity, group of entities or any other person or organisation. This may include manipulation of the content of a policy or approval or manipulating the process of policy development or approval. There is a risk that sensitive information is inappropriately shared or accessed or compromised.’

70 APRA’s risk register identified: ‘Supervisory Fraud Risk – Deliberate manipulation of supervisory decision or the enforcement and investigations process for personal gain, also includes bribery and corruption. Includes all supervision related decisions e.g. approvals, licensing and policy interpretations. An APRA employee deliberately manipulates a supervisory decision for personal gain or to cause a loss to an entity or any other person. Includes manipulation of supervisory decision to cause an impact to APRA’s reputation, impact the entity in any way or to cause a market impact.’

71 APRA also advised the ANAO in March 2023 that there was a focus on ‘grooming’ in October 2022. In this context, grooming refers to ‘the deliberate targeting and intentional manipulation of APRA employees, contractors, consultants and secondees by others to obtain an illegitimate or illegal advantage’. APRA further advised that ‘the Chair recommended all employees watch a video supplied by the ACLEI [Australian Commission for Law Enforcement Integrity] on a case study of an APS [Australian Public Service] employee being groomed by a regulated entity. There were over 240 views of the video at the time. This was followed up with an all staff ... panel session with one of the Executive Directors and an ACLEI representative – this had 347 attendees’. An article was also published on APRA’s intranet in relation to grooming, which was promoted by the Chair in an all staff message.

2.33 APRA advised the ANAO that it has arrangements that demonstrate APRA has identified regulatory capture risk and established arrangements to mitigate against the risk. APRA advised that these include the following.

- The introduction in June 2022 of supervision tenure⁷² guidance across APRA's Banking, Insurance and Superannuation divisions. The guidance states that 'A supervisor's tenure on an entity portfolio should not exceed 5 years.'⁷³
- Financial and non-financial conflicts declaration (as discussed in paragraphs 2.10 to 2.25).
- Supervisory approval and oversight arrangements.⁷⁴
- Fraud control arrangements, which include an anonymous reporting line for both employees and persons outside of APRA.⁷⁵

2.34 The ANAO did not assess whether the identified risks relating to regulatory capture were effectively managed by APRA.⁷⁶

2.35 The Parliamentary Joint Committee on Corporations and Financial Services has identified regulatory capture as a significant issue faced by Australian regulators, and the attendant risks have been acknowledged by APRA. Given the significance of the risk, there would be benefit in APRA addressing regulatory capture risk and its management, in the entity corporate plan.

72 APRA's Supervision Tenure guidance (June 2022) states that: 'Supervision tenure refers to the length of *continuous time* spent by a responsible analyst, responsible supervisor or leaders up to and including General Managers, on the supervision of an entity or group of entities (entity portfolio). Periodic review of supervisory tenure on an entity portfolio not only mitigates the risk of regulatory capture and supervision risk captured under APRA's Risk Appetite Statement ... it also provides development opportunities and the benefit of a new perspective and diverse views.'

73 The guidance states that: 'Approval by the relevant industry Executive Director (ED) is required for any extension beyond 5 years, with a maximum transition period of up to 12 months. Extensions will only be granted in extenuating circumstances, such as finalisation of a complex issue, remediation program, a merger which is in train or the departure of a key person. Where a supervisor has held an entity portfolio for 5 years or more, the supervisor will be unable to resume the same entity portfolio for a minimum of 3 years. Exceptions may be granted in extenuating circumstance with the approval of the relevant ED.'

APRA documentation states that Supervision Divisions will have until 30 June 2023 to comply with the guidance. APRA advised the ANAO that in some cases there are supervisors who have been assigned entities for more than five years and that these cases will be resolved over the next 12–18 months. APRA further advised the ANAO that: 'a) mitigation strategies are in place to reduce the risk and decisions made to retain the supervisors in the short-term; b) we've had regard to important considerations such as stability and ensuring the entity remains effectively supervised; c) we also consider other factors such as the level of executive turnover at the entity itself; and d) where a supervisor has spent more than five years on one entity, the extension has Executive Director approval and there is a plan in place for sensible transition.'

74 For example, APRA advised the ANAO that: 'There are layers of approval and oversight for key decision points within supervision teams across APRA's supervision divisions to prevent unilateral or unusual decision making on material issues. In addition there are prescribed levels of delegation for decisions which are contained in APRA's enabling legislation, and these are recorded and reviewed quarterly.'

APRA further advised the ANAO that it has in place a Supervision Oversight Committee. The purpose of this committee includes: contribute to material supervisory decisions with senior input and advice; and oversee core supervisory functions, assess their effectiveness and implement necessary enhancements.

75 APRA's fraud management arrangements are discussed in paragraphs 2.104 to 2.111.

76 The ANAO reviewed the extent to which regulatory capture risk was reflected in APRA's key external corporate documents and internal risk documentation as part of reviewing, at a high level, whether APRA had identified regulatory capture as an enterprise risk.

Opportunity for improvement

2.36 There is an opportunity for the Australian Prudential Regulation Authority to consider including references to regulatory capture risk and how it is managed in the entity corporate plan.

Financial Holdings Disclosure

2.37 In addition to general conflict of interest risk (discussed in paragraphs 2.10 to 2.25) and regulatory capture risks, APRA has identified a specific entity-wide risk relating to APRA officials inappropriately gaining financial advantage due to their role at APRA. Specifically, APRA employees are expected to not have, or be seen to have, any conflict between their obligations to supervise regulated financial institutions in the public interest, and their private financial interests in those institutions, or other dealings or arrangements with APRA-regulated institutions that are not a commercial arm's length arrangement.

2.38 APRA developed a Financial Holdings Disclosure Policy (FHD policy), dated September 2021⁷⁷, and established procedures and arrangements intended to manage this identified risk. The FHD policy references APRA's Code of Conduct, which requires APRA Members and staff, among other things, to:

respect confidential, personal or sensitive information you have access to and do not take advantage of, or allow others to take advantage of, information or knowledge obtained during the course of your employment;

...

avoid any conflict of interest (real or perceived) in connection with your employment, including disclosing internal or external personal relationships that may be perceived as a conflict of interest;

...

disclose any equity holdings you have in APRA-regulated entities and abide by the Staff Disclosure of Interests Policy regarding acquiring financial holdings ...

2.39 The 2021 FHD policy states that:

This Policy is to be read in conjunction with APRA's Conflicts of Interest (CoI) Framework which is the overarching document supporting this Policy ...

As APRA is the prudential regulator of the financial sector, it is important that all APRA employees should not have, or are not seen to have, any conflict between their obligations to supervise regulated financial institutions in the public interest, and their private financial interests in those institutions, or other dealings and arrangements with an APRA-regulated institution that are not a commercial arm's-length arrangement or other relationship that could be seen to create a conflict of interest ...

The COI Framework including the Financial Holdings Disclosure Policy applies to any person acting on behalf of APRA including APRA Members, full and part-time employees of APRA, contractors, secondees or any other individual with access to APRA's systems and records. For ease of reference, all of these are referred to as 'employees' for the purposes of the Framework and associated policies and procedures.

⁷⁷ For part of the period subject to ANAO review, an earlier version of APRA's FHD policy was in place. The previous version was issued in April 2019 and was broadly similar in nature to the September 2021 version.

2.40 The 2021 FHD policy, among other things, requires employees to disclose equity holdings when they commence at APRA and not acquire equity holdings⁷⁸ in APRA-regulated institutions.⁷⁹

2.41 The 2021 FHD policy states that:

APRA's policy in relation to financial interests is as follows:

(i) APRA employees must not improperly use or disclose information obtained in the course of their work at APRA. This obligation is imposed on all employees under APRA's Code of Conduct, the relevant provisions of the APRA Act (secrecy provisions), the Corporations Act (including insider trading or tipping prohibitions), the Criminal Code Act (secrecy of information) and the common law. For the avoidance of doubt, this general principle applies to all financial interests and is not limited to financial interests in APRA-regulated institutions.

(ii) Employees will be required to regularly attest their understanding of APRA's Code of Conduct and the COI Policies which cover various statutory provisions (both civil and criminal) prescribing their obligations regarding honesty, protection of confidential information and insider trading. In relation to financial holdings it is also important to note that insider trading provisions (as prescribed by the Corporations Act) apply under APRA's Code of Conduct.

2.42 A declaration of interest must be completed by employees on joining APRA.⁸⁰ The 2021 FHD policy states that: 'Employees are also required to disclose on a "best of knowledge" basis the holdings of their "immediate family."' ⁸¹ In addition, 'Employees must disclose the number of equity holdings in any APRA-regulated institutions in which they have an interest.' Employees may not

78 Equity holdings are defined in the policy as including:

equity derivatives and all tradeable securities:

- a. which create an equity interest or potential equity interest in an APRA regulated entity (or close associates of regulated entities);
- b. which carry a right to vote; or
- c. the return on which will vary according to the entity's profitability, among other factors.

These include, but are not limited to, shares of all classes, options, futures, warrants, debt instruments, hybrids and any other interest that derives from the shares of an APRA-regulated entity. For the avoidance of doubt, this includes entering into any agreement to borrow or acquire equity interests at a future date, e.g. in the case of a short sale.

Employees should consult with the relevant ED in relation to proposed investments in emerging investment instruments, or where they are unsure of the nature of the investment in terms of compliance with this policy.

79 The policy also states that: 'APRA employees may continue to maintain equity holdings in APRA-regulated institutions held at the time they commenced work at APRA, provided such interests are fully disclosed and managed in accordance with this policy.'

80 As discussed in paragraph 2.20, new starters at APRA are required to complete the Conflicts of Interest Declaration within one month of joining APRA. APRA's Framework document (discussed in paragraph 2.14) states that: 'Any equity holdings declared in the COI [conflict of interest] form will be auto-populated into the Financial Holding form. Any subsequent changes or approval requests should be updated via the Financial Holding form.'

81 Immediate family is defined as including 'the spouse (including de facto spouse), partner and dependent children of the APRA employee.' In addition, the policy states that 'transactions made on behalf of an employee by their financial advisors are subject to this policy and employees are required to inform their financial advisors, in writing, of the restrictions of this policy'.

acquire additional holdings except as a direct consequence of passive activities⁸² and ‘such additional holdings must be fully declared as soon as the employee becomes aware of the entitlement.’ The policy further states that:

(ix) If a conflict arises (or becomes apparent from the employee’s disclosure of interests), the relevant Executive Director (ED) may re-assign the employee to a position not carrying the same conflict, or request that the holdings be divested.

(x) Employees wishing to sell existing equity holdings should consult with their ED in advance, specifying the reasons for the proposed sale, and indicating whether the sale represents a full or partial disposal of their holdings in the entity. After consulting with their ED, the staff member should submit a formal request for their ED’s approval via the Financial Holding form in APRA’s conflicts management system ...

2.43 The policy further states that:

If the ED [Executive Director] judges that such a sale is likely to create a perceived/actual conflict they can, in writing, request that it not proceed, or impose conditions on when the sale is to occur (for example in a pre-determined trading window).

2.44 If approved, the approval remains valid for a maximum of three business days and employees are to confirm the sale immediately after it occurs. Executive Directors wishing to sell existing equity holdings must obtain approval from the APRA Member to whom they report; and APRA Members wishing to sell equity holdings must obtain the approval as set out in APRA’s approval protocol for Members.⁸³ Any approval must also be advised to the Chair of APRA’s Audit and Risk Committee. Employees must keep their financial holding declaration current and notify their relevant Executive Director immediately when changes occur or when approval is required.

2.45 As outlined in paragraph 2.20, APRA employees are required to submit an annual conflicts of interest declaration on joining APRA and this declaration must be updated annually. APRA’s arrangements for annual attestation of financial holdings disclosure are discussed in Chapter 4 of this audit in paragraphs 4.8 to 4.12.

82 For example, demutualisations, share splits, bonus shares, script-based takeover offers or the exercise of options with a pre-existing end date or dividend reinvestment plans. The exercise of entitlements such as participation in dividend reinvestment plans, rights to acquire additional shares and share purchase plans, will only be permitted in circumstances where the entitlement was pre-existing at the time of joining APRA. Funds that do not provide for investor choice over the specific individual investments within the fund, that include APRA-regulated institutions (or close associates of regulated institutions), are permitted.

83 Members wishing to sell equity holdings must obtain the relevant approval. They must follow the approval protocol for Members using the ‘circular approval’ process, whereby each Member has a nominated approver and Members cannot approve a Member who is assigned to approve them.

APRA advised the ANAO in January 2023 that the APRA Chair is advised, when a Member sells or acquires equity holdings, via Risk Management and Compliance reporting. APRA further advised that biannually the Chair is advised of the conflicts of interest disclosures (including financial holdings) of all Members by reporting from APRA’s Risk Management and Compliance team. This includes any change in holdings, which are highlighted. The reports are sent in January and August. The Chair’s contemporaneous approval for the sale of shares is not required. The approval requirement follows the Member’s finance approval protocols. The Audit and Risk Committee Chair needs to be advised of any sale approval. Under arrangements with the Department of the Treasury, the Treasurer is required to be advised of any changes of Members’ disclosed interests, hence the Chair is included/advised of all communications to the Treasurer.

Information security

2.46 In the course of undertaking its regulatory functions, APRA collects, analyses, shares and stores sensitive and confidential information. APRA's security policy addresses the confidentiality of information security, stating that: 'Information is observed by or disclosed to only those who have a need to know'.

2.47 APRA's December 2022 risk appetite statement includes risks to organisational effectiveness, as follows: 'The delivery of APRA's purpose and vision is at risk from failing to maintain robust and efficient practices, systems and premises.' The risk appetite statement observes that APRA has a very low tolerance for 'material instances of inappropriate disclosure of confidential/sensitive information in the course of performing its activities'.⁸⁴

2.48 APRA's Executive Committee receives reporting on these identified risks, including on the effectiveness of controls in place to manage them. APRA's Executive Committee also receives a security update twice a year, which includes reporting on information security risks.

2.49 APRA has documented that its information security arrangements include monitoring of: email traffic to personal email accounts; the use of USB (portable storage) devices; and 'information security reportable incidents' in APRA's risk management system.⁸⁵ APRA advised the ANAO in January 2023 that in response to a gap identified as part of APRA's 2021–22 Protective Security Policy Framework⁸⁶ maturity assessment submitted in October 2022, from November 2022 a new cessation process and clearance form was introduced. Under the new process, all departing employees are required to complete and have an appropriately approved Cessation Clearance Form that outlines post-employment obligations in relation to section 56 of the APRA Act.⁸⁷

Senior executive remuneration

Entity policy

2.50 A senior executive remuneration policy contributes to the management of probity within an entity by introducing transparency in the remuneration setting process. Having the accountable

84 APRA's previous risk appetite statement (effective from November 2020 to December 2022) documented a nil appetite for the equivalent risk, and included a note stating:

APRA recognises the practical constraints of fully preventing these risks from materialising. However, if a risk outside of Nil appetite materialises, APRA commits to timely action, including investigation and where considered appropriate, remediation.

APRA records indicate that all risks with a 'nil' appetite were changed to 'very low' in the November 2022 review of APRA's risk appetite statement.

85 Information security reportable incidents include emails sent to incorrect addressees.

86 Attorney-General's Department, *Protective Security Policy Framework (PSPF)* [Internet], AGD, available from <https://www.protectivesecurity.gov.au/> [accessed 21 November 2022].

The PSPF applies to non-corporate Commonwealth entities subject to the PGPA Act to the extent consistent with legislation. The PSPF represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies under the PGPA Act. Non-government organisations that access security classified information may be required to enter into a deed or agreement to apply relevant parts of the PSPF for that information.

87 The cessation clearance form requires the official to acknowledge that the secrecy obligation imposed under section 56 of the APRA Act 'does not end when you leave APRA.' Officials are advised that 'You still must not divulge any information, or provide any documents, relating to an entity regulated by APRA to anyone, unless the information or documents are already public. Breach of this obligation could result in prosecution and a penalty of two years imprisonment. Unlawful disclosure of information might also be a breach of the Crimes Act 1914, which also carries a penalty of two years imprisonment.'

authority establish and approve remuneration policies also enables the accountable authority to influence behaviour and can be an important mechanism in communicating the desired culture within the entity.

2.51 For the period examined as part of this audit, APRA did not have a policy that set out remuneration requirements in relation to its senior executives.

2.52 APRA has a Remuneration Review Policy (dated June 2022) which outlines the basis and process by which APRA reviews remuneration for non-senior executive staff. APRA advised the ANAO that while the policy does not apply formally to senior executives, in practice it is applied to them, and remuneration review processes are the same for staff and senior executives. The policy does not state that it applies to senior executives and not all the steps in the policy are applicable to the senior executive cohort. To improve transparency, APRA should either clarify which parts of the policy apply to senior executives or issue a specific remuneration policy for senior executives. The latter option would maximise transparency.

Recommendation no. 1

2.53 The Australian Prudential Regulation Authority develop and issue a remuneration policy for its senior executives.

Australian Prudential Regulation Authority response: *Agreed.*

2.54 *APRA formally applies the Remuneration Review Policy (June 2022) to senior executives. APRA will review the Policy and include appropriate provisions to explicitly note its application to senior executive employees.*

Government policy

2.55 Probity requirements for the personnel of Australian Government entities include compliance with applicable laws and government policies.⁸⁸

2.56 In recent years the Australian Government has made decisions that impacted remuneration arrangements for senior executives in Australian Government entities. On 26 March 2020, the Australian Government announced that all remuneration increases for Australian Public Service (APS) Senior Executive Service (SES) or equivalent employees (senior executives) would be suspended across the Commonwealth public sector in response to the COVID-19 pandemic.⁸⁹ On 25 June 2021, the Australian Public Service Commission (APSC) announced the end of the pause on all remuneration adjustments for senior executives.⁹⁰ APRA records indicate that it applied the

88 For example, section 21 of the PGPA Act provides that the accountable authority of a non-corporate Commonwealth entity must govern the entity in a way that is not inconsistent with the policies of the Australian Government.

89 The suspension applied to general wage increases and, where applicable, performance-based increment progression plus payment of discretionary SES bonuses.
Australian Public Service Commission, *Australian Public Service Remuneration Report 2021* [Internet], APSC, p. 2, available from <https://www.apsc.gov.au/sites/default/files/2022-08/Australian%20Public%20Service%20-%20Remuneration%20Report%202021%20-%20Accessible.pdf> [accessed 28 October 2022].

90 *ibid.*

March 2020 remuneration pause to its senior executives and there were no pay increases for the 2019–20 financial year.

2.57 In August 2021 the APSC released *Performance Bonus Guidance* applicable to all Commonwealth entities and companies. The guidance stated that:

Commonwealth entities and companies should exercise rigour and restraint in the use of performance bonus payments ... Performance bonuses may only be used in limited circumstances, justifiable to the Parliament and the public ... As a general principle, most positions should not be eligible to earn a performance bonus. For instance, performance bonuses would not be appropriate in most policy, service delivery, regulatory, or corporate roles ... Commonwealth entities and companies should avoid the broad use of performance bonuses.⁹¹

2.58 Following this advice, APRA undertook to roll performance bonuses into remuneration for all APRA staff, including its senior executives. APRA documentation indicates this was in recognition that future remuneration reviews would no longer include bonus payments and would result in a one-off uplift to remuneration. This resulted in a 5.5 per cent increase in total remuneration for all eligible APRA employees.⁹² APRA advised the ANAO that:

Though the 5.5% increase was not guaranteed to Senior Executives such as GMs [General Managers] (who are employed on Senior Contracts and not the APRA Enterprise Agreement), there was a decision taken by APRA Members to apply this guaranteed component to this cohort as this was intended to buy out the performance bonuses, which had also been approximately 8% on average for this cohort.

2.59 The 5.5 per cent increase in remuneration formed part of an overall average increase of 9.2 per cent for APRA Executive Directors and nine per cent for APRA General Managers. The part not related to the roll-in of performance bonuses related to ‘capability of the individual (including performance and progression) and other market factors such as internal and external market relativities’ assessed as part of APRA’s annual review of remuneration.

2.60 APRA’s Remuneration Review Policy (dated June 2022), which APRA has advised applies to all staff, states that:

Remuneration reviews will be conducted annually and take into account an employee’s capability in role, role scope, complexity, and internal and external benchmarking ...

APRA will review an employee’s remuneration based on:

- a. market considerations of the role and salary benchmarking, to both external industry and internal peers;
- b. scope and complexity of their role;
- c. depth of knowledge in terms of industry, market trends and application of this to role;
- d. demonstrated ability to adapt to changing needs of the role and organisation;

91 Australian Public Service Commission, *Performance Bonus Guidance* [Internet], APSC, 13 August 2021, p. 2, available from <https://www.apsc.gov.au/circulars-guidance-and-advice/performance-bonus-guidance#downloads> [accessed 28 October 2022].

92 APRA advised the ANAO that this was made up of ‘4% roll-in of performance bonuses to base remuneration, plus the 1% guaranteed element of the WPI [wage price index] budget as detailed in the Enterprise Agreement, plus 0.5% pass on of SGC [superannuation guarantee charge]. If the employee did not complete a full 2021-22 year the amount was pro-rated.’

- e. skills being aligned with APRA's strategy and considered critical for future success; and
- f. evidence of proactively seeking out opportunities and building internal and external relationships to promote collaboration.

2.61 APRA documentation indicates that it reviewed the performance of members of the senior executive having regard to capability, the nature of their role and internal and external benchmarks.⁹³ There is also evidence that the APRA Chair was provided with details of remuneration arrangements for the senior executive cohort. Further details are discussed in Chapter 4 of this audit in paragraphs 4.13 to 4.20.

Procurement

2.62 APRA has identified key probity risks related to procurement and has developed policies, procedures and arrangements to manage the identified risks.

2.63 Under the PGPA Act, the Finance Minister issues the Commonwealth Procurement Rules (CPRs) for officials to follow when performing duties in relation to procurement. The CPRs govern how entities buy goods and services and state that procurements should:

use public resources in an efficient, effective, economical and ethical manner that is not inconsistent with the policies of the Commonwealth.⁹⁴

2.64 The CPRs define the terms 'efficient', 'effective', 'economical' and 'ethical', and state that:

Ethical relates to honesty, integrity, probity, diligence, fairness and consistency. Ethical behaviour identifies and manages conflicts of interests, and does not make improper use of an individual's position.⁹⁵

2.65 Under the CPRs, ethical behaviour includes:

- recognising and dealing with actual, potential and perceived conflicts of interest;
- dealing with potential suppliers, tenderers and suppliers equitably, including by seeking appropriate internal or external advice when probity issues arise, and not accepting inappropriate gifts or hospitality;
- carefully considering the use of public resources; and
- complying with all directions, including relevant entity requirements, in relation to gifts or hospitality, privacy and security.⁹⁶

2.66 The APRA Chair's Finance Instructions and Policies (CFIs) identify that APRA is required to comply with the CPRs. APRA's procurement guidance does not specifically mention probity or include additional specific operational requirements for the management of probity in procurement

93 APRA documents do not explicitly demonstrate consideration of factors c-f as listed in paragraph 2.60.

94 Department of Finance, *Commonwealth Procurement Rules Finance* [Internet], Finance, 1 July 2022, p. 11, paragraph 4.4, available at: <https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules> [accessed 21 November 2022]. The CPRs are subject to periodic update.

95 *ibid.*, p. 15, paragraph 6.5.

96 *ibid.*, p. 15, paragraph 6.6.

Additionally, the Department of Finance has issued guidance outlining 11 principles to support probity in procurement. These are included in Appendix 3 of this audit report.

including in relation to entities APRA regulates. In March 2023 APRA advised the ANAO that it does not procure from the entities it regulates.⁹⁷

2.67 In January 2022, APRA undertook an internal audit titled ‘Procure-to-Pay’. In the final report APRA’s control environment was rated as ‘Needs improvement’ and management awareness was rated as ‘Satisfactory’. The report included two overall findings that relate to probity, which were rated ‘amber’.⁹⁸ These findings related to fraud controls and procurement activities.⁹⁹ The rating rationale for the procurement finding was that: ‘These weaknesses impact on transparency and probity, which could lead to perceptions of improper process and impact APRA’s reputation.’

2.68 APRA advised the ANAO in November 2022 that in response to the internal audit findings, in February 2022 APRA introduced a further step in the procurement process — when a procurement request is made in APRA’s system, the requestor must complete a check box to ‘confirm that should anyone involved in the selection process, have any pecuniary or non-pecuniary conflicts of interest with any of the suppliers being evaluated for this procurement, I will notify Procurement immediately.’ APRA further advised the ANAO in March 2023 that its central procurement team maintains records of any conflict of interest declarations and decisions. The introduction of this check box enables APRA to demonstrate consideration of conflict of interest.

2.69 For some procurements, an ‘evaluation methodology’ document is prepared, which requires signatures from evaluation team members and a member of APRA’s procurement team. Versions of this document seen by the ANAO include statements regarding evaluation team members’ obligations to ‘advise the Procurement Team of any pecuniary or non-pecuniary interests they have in any Respondent submitting proposals in response to the RFT at the first reasonable opportunity.’

2.70 The ANAO examined a sample of APRA procurements (see paragraphs 4.21 to 4.26) and found that for some procurements, members of the evaluation team were asked to provide activity-specific conflict of interest declarations.

2.71 In summary, the ANAO observed variance in approach within APRA. There is an opportunity for APRA to obtain greater consistency in its identification and management of probity risks by enhancing its guidance in relation to the management of probity risks in procurement.

97 APRA also advised the ANAO that there may be instances where a regulated entity is consulted to ensure investigations do not have conflicts of interest.

98 APRA internal audit reports have colour-coded risk ratings: green, yellow, amber and red, escalating from the lowest risk rating (green) to the highest rating (red).

99 The two amber findings were that APRA implement additional controls to mitigate fraud risk and strengthen practices to demonstrate that fair and transparent actions are undertaken across all procurement activities. In relation to procurement the audit made a number of detailed findings including that: there was no evidence of consideration of conflict of interest for procurements less than \$80,000; there was a high exception rate (67 per cent) to meeting APRA’s requirements to obtain three quotes for procurements valued between \$20,000 and \$80,000; and APRA’s tender evaluation methodology did not specify that no changes should be made to evaluation methodology after tenders had opened. APRA records indicate that the remediation action for the first finding (the most relevant to this ANAO audit) was to ‘Revise Procurement’s SHOP [APRA’s Service and Help Online Portal] ticket request form to ensure business users actively account for any potential Conflicts of Interest in the transaction.’ There is evidence that this has been implemented.

Opportunity for improvement

2.72 There is an opportunity for the Australian Prudential Regulation Authority to improve consistency in its identification and management of probity risks in procurement by establishing guidance that details:

- probity management requirements applicable to all procurements; and
- the circumstances that require additional probity management measures, and what those additional probity management measures are.

Corporate credit card expenditure

2.73 APRA has identified the key probity risks related to corporate credit card expenditure and developed policies, procedures and arrangements to manage the identified risks.

2.74 Corporate credit cards (credit cards) offer a transparent, flexible and efficient way for Australian Government officials to obtain cash, goods or services to meet business needs. Australian Government policy requires non-corporate Commonwealth entities to pay expenses via a payment card where the payment is an eligible payment under \$10,000.¹⁰⁰ The misuse of credit cards can expose an entity to risks such as waste and fraud. Instances of misuse and weaknesses in relevant entity controls attract considerable parliamentary and public interest and can cause reputational damage to affected entities and the Australian Government.¹⁰¹

2.75 APRA issues credit cards to Members and staff.¹⁰² The ANAO reviewed APRA's credit card policy, procedures and arrangements to assess whether they addressed selected risks associated with the use of credit cards. In particular, the ANAO examined whether APRA's policies, procedures and arrangements addressed:

- requirements for the issue of credit cards, including specifying cardholder obligations;
- expenditure approval requirements;
- acquittal requirements (including timing and documentation requirements and reviewer responsibilities); and
- requirements for the return of credit cards.

2.76 APRA's credit card policy is contained within APRA's CFIs (August 2022) and applies to all APRA corporate credit cardholders. APRA also provides credit card related guidance on its intranet.

¹⁰⁰ The value is inclusive of GST and merchant service fees.

Department of Finance, *Payment card policy for payments valued below \$10,000* [Internet], Finance, July 2022, available from <https://www.finance.gov.au/publications/resource-management-guides/supplier-pay-time-or-pay-interest-policy-rmg-417/part-2-payment-card-policy-payments-valued-below-10000> [accessed 1 November 2022].

¹⁰¹ Auditor-General Report No.8 2016–17 *Controls over Credit Card Use*, p. 13.

¹⁰² APRA advised the ANAO that contractors can apply for a card if there is a business case for them to have one, but this is rare.

Requirements for the issue of credit cards including specifying cardholder obligations

2.77 APRA's intranet guidance sets out the application process, which includes the requirement to meet application criteria¹⁰³, agree to comply with terms and conditions¹⁰⁴ and obtain cost centre manager approval for a card to be issued. The policy sets out the requirements and responsibilities in relation to the management and use of credit cards and states that: 'In appointing a card provider consideration will be given to any conflicts of interest APRA may have with Regulated Entities.'

Credit card expenditure limits

2.78 APRA has established transactional and monthly limits on all APRA credit cards. Different limits apply based on the role of the cardholder. The limits are listed in Table 2.1.

Table 2.1: APRA corporate credit card limits

APRA role	Value per transaction (\$)	Value per month (\$)
Levels 1–4	5,000	20,000
Senior Manager (Level 5) General Manager Executive General Manager	20,000	30,000
Member	20,000	60,000

Source: ANAO analysis of APRA documentation.

2.79 Under APRA's CFIs, credit card holders have prior expenditure approval up to the limit of their credit card through the Instrument of Delegation, and 'All expenditure above the delegation Credit Card limit will be approved by the relevant CCM [Cost Centre Manager] prior to the expense being incurred on the Credit Card.'

Expenditure approval requirements

2.80 The credit card policy states that: 'The APRA Credit Card will not be used for private expenditure at any time, even if promptly repaid. Such usage is a breach of the PGPA Act and will be reported to the Members via the compliance monitoring processes.'¹⁰⁵ The policy also states that: 'In the event a Credit Card is misused by an Official, the cardholder will be responsible for reimbursing APRA for the expense within the statement period.'

2.81 The issuing of a corporate credit card to a staff member is approved by a cost centre manager. Credit card holders then have prior expenditure approval up to the limit of their credit card, details of which are in Table 2.1. Additional guidance on the APRA intranet sets time limits for submitting and approving transactions.

103 Applicants must need either to: make at least one purchase, or travel on behalf of APRA on one occasion, in the next 12 months; or the employee manages a team and the team will likely utilise the corporate credit card to make at least one purchase on behalf of APRA in the next 12 months.

104 These include ensuring that: the card is only to be used for official purposes; credit card use is consistent with relevant delegations and complies with relevant APRA policies and procedures; the credit card must be kept safe at all times; and the cardholder meets acquittal requirements.

105 The policy states that: 'Charges to the Credit Card are considered expenditure of public money and will meet the criteria set out in the 'Spending Public Money' policy. At the point of purchase, any private elements will be settled separately by the Official.'

Approval arrangements for APRA Members

2.82 A corporate credit cardholder's expenditure is typically approved by their supervisor. For the role of the accountable authority there is a power imbalance as they do not have the equivalent of a supervisor. Previous ANAO audits have identified risks in relation to positional authority.¹⁰⁶ In Auditor-General Report No.22 2015–16 *Defence's Management of Credit and other Transaction Cards*, the ANAO reported that for review of credit card transactions to work effectively:

the reviewer must be in a position to exercise independent judgement ... this means that they cannot be in a position which would constrain unreasonably their capacity to question transactions that appear inappropriate; for example, this may be difficult for a person junior to the cardholder ... (paragraph 2.42).

2.83 The 2020 Thom review of the Australian Securities and Investments Commission (ASIC) governance arrangements¹⁰⁷ also highlighted risks related to positional authority when approving expenses for very senior personnel. The report stated that:

Clearly there are particular challenges that arise when subordinate officials are required to approve expenses for very senior statutory officers, particular for the Accountable Authority. These decisions can still be problematic, even if the approving official is very senior, for example, the CFO or COO ... challenges arise for expenses that, while business expenses in nature, have sensitivities and can be subject to public scrutiny and criticism.¹⁰⁸

2.84 Recommendation 8 of the Thom review included the following elements, to manage positional authority issues related to expense approvals.

The review recommends that ASIC should:

...

- Require the Chair's approval for the expenses of Commission members; and
- Require a Deputy Chair's approval for the Chair's expenses.¹⁰⁹

2.85 Although directed to ASIC, the recommendation highlighted a risk for statutory bodies. APRA documentation indicates that the APRA Chair advised APRA Members of approval arrangements to be observed for their expenses, effective from 1 July 2021. These arrangements are documented and referred to as APRA's 'circular approval' arrangements. They involve the Chair

106 For example, Auditor-General Report No.1 2021–22 *Defence's Administration of Enabling Services — Enterprise Resource Planning Program: Tranche 1*, paragraphs 4.30 and 4.42, discussed risk relating to positional authority in relation to delegation and time approval arrangements.

107 The review related to ASIC, one of the three Australian Government regulators examined in this ANAO audit series on probity management. The review included recommendations directed to ASIC on its policies relating to the payment of Commissioner expenses and related controls. An abridged public version of the report was released in 2021.

108 Dr Vivienne Thom AM, *Abridged report on the review of ASIC governance arrangements* [Internet], Department of the Treasury, 28 January 2021, p. 39, available from https://ministers.treasury.gov.au/sites/ministers.treasury.gov.au/files/2021-01/Abridged_ASIC_Governance_Report-for-release_0.pdf [accessed 24 March 2023].

109 *ibid.*, Recommendation 8, pp. 6-7.

and each Member having a different designated approver for their expenses.¹¹⁰ Under APRA's arrangements, the Deputy Chair approves the Chair's expenses. However, not all Member expenses are approved by the APRA Chair, and expenses can be approved by peers. This approach is not consistent with that recommended by the Thom review. There is an opportunity for improvement for APRA to consider the adoption of that approach.

Opportunity for improvement

2.86 There is an opportunity for the Australian Prudential Regulation Authority to reduce positional authority risk by providing that all APRA Member expenses are approved by the APRA Chair.

2.87 In respect to executive assistants, APRA advised the ANAO that:

Executive Assistants have their own credit cards which they use to make purchases for Members such as ad hoc office supplies (stationery) or for refreshments for meetings etc. These expenses are approved by their Manager (the Member themselves).

In addition, Executive Assistants can make purchases on behalf of Members (example book a flight for one of the Members) using the Member's CC [credit card]. However, this would still need to follow the existing Circular Arrangements in place for approval purposes (i.e., the transaction needs to be approved by the designated alternate Member).

Acquittal requirements

2.88 APRA's credit card policy and guidance set out acquittal requirements including timing and documentation requirements. The acquittal process for credit card transactions is undertaken online. Cardholders (or a proxy¹¹¹) are required 'to complete transactions and submit to Cost Centre Manager/Delegate for online approval' by a specified date (the 15th of each month). The policy states that:

Cardholders are requested to obtain receipts/tax invoices for all appropriate transactions/charges. Expenditure items over \$82.50 (Including GST) must be supported by a Tax Invoice.

2.89 APRA's intranet credit card guidance provides some guidance on requirements regarding lost tax invoices. In addition, a User Guide from APRA's Finance team states that:

Where substantiation is not possible (e.g. tax invoices are misplaced/lost) suitable justification / explanation will need to be provided to the acquitting manager. It is up to the acquitting manager whether they will approve the expense in this situation. It is expected that the acquitting manager will counsel the card user on the need for always providing the necessary substantiation for all transactions made, and the acquitting manager may reject such a claim if substantiation is repeatedly not provided. Finance no longer require a statutory declaration to be provided. Any

110 An alternate Member may approve expenses in the event the designated approving Member is unavailable, for example due to being on leave. In such cases: the Member seeking approval should not be the approver of the alternate's expenses; if two Members are on leave, the remaining two Members may approve each other's expenses; and APRA's Finance area is required to be advised of the use of these exception arrangements. Documentation also references that in addition to the approval arrangements outlined, Internal Audit will conduct a six monthly review and audit of all Member expenses (referred to in paragraph 2.92). Any 'questionable items' identified by Finance or Internal Audit will be discussed with the Chief Operating Officer or Chief Internal Auditor and either resolved with the Member(s) concerned or raised with APRA's Audit and Risk Committee.

111 APRA's credit card guidance states that: 'Cardholders can nominate a "Proxy" to access/view their statement on their behalf'. A typical proxy would be the executive assistant of a senior manager or APRA Member.

transactions without substantiation will be recorded in the finance register of missing substantiation and reported to the EDs on a half-yearly basis.

Acquittal arrangements for APRA Members

2.90 APRA has not documented its acquittal arrangements for APRA Members. APRA advised the ANAO that 'Credit card acquittals for Members are actioned by either the Member or their Executive Assistant' and acquittal approval is 'in line with the circular arrangement'.

Requirements for the return of credit cards

2.91 APRA's intranet guidance outlines requirements when cardholders leave APRA or go on extended leave.¹¹² The guidance also states that APRA management may decide to suspend a card at any time for misuse or non-acquittal. The terms and conditions for obtaining a card also require that cardholders must surrender the credit card upon request.

APRA monitoring of credit card use

2.92 APRA's Internal Audit unit has conducted two bi-annual probity reviews of APRA Members' credit card transactions, for compliance and reasonableness.¹¹³ These reviews have identified examples of acquittal, approval and expenditure substantiation actions not meeting APRA requirements.¹¹⁴ The results were reported to APRA's Executive Board. The Board minutes record that:

The EB [Executive Board] discussed the issues surrounding the observations and agreed a tightening of the process, including ensuring the Members' Executive Assistants were fully aware of the requirements, was necessary. **Action:** The Executive Office to liaise with Internal Audit and Finance to address the underlying issues regarding the approval of Members' expenses [emphasis in original].

2.93 APRA's CFI states that, in relation to credit cards:

Regular management reports relating to the use of Credit Cards will be run from the Financial Management Information System (FMIS) and/or the card provider's systems and anomalies will be actioned on a monthly basis by Finance.

112 For example, a card will be cancelled when a cardholder leaves, is on parental leave or takes extended leave without pay (more than six months).

113 The first report was issued in February 2022 and covered the period 1 February 2021 to 30 November 2021. The second report was issued in August 2022 and covered the period 1 December 2021 to 31 May 2022.

114 The August 2022 report identified that:

- Thirty six per cent of transactions were acquitted late with an average of 32 days late (compared to 17 per cent in the prior period with an average of 43 days late).
- Two per cent of transactions were approved late with an average of 46 days late (compared to 12 per cent with an average of 17 days late in the prior period).
- Seven transactions from one APRA Member with a combined value of approximately \$9,600 were approved by an APRA General Manager (who is a subordinate to an APRA Member) rather than the APRA Chair as required.
- A further 11 transactions were not approved in accordance with APRA's circular approval requirements for APRA Members. They were instead approved by an alternate Member. Seven of these 11 transactions were approved by the APRA Chair.
- Six instances were identified where transactions over \$82.50 were not supported by a tax invoice as required.

2.94 APRA documentation also indicates that APRA's Finance team performs an annual analysis and review of all credit card transactions periodically during the financial year. This review is performed to ensure proper use of corporate credit cards and public monies.

2.95 APRA records indicate that the Finance team conducted the following credit card analysis.

- A review of transactions from October 2020 to December 2020. The results were reported to APRA's Head of Finance in July 2021. APRA documentation records that 312 transactions were reviewed, with a total value of \$83,111. Fourteen transactions, with a combined value of \$739, were identified for further investigation.¹¹⁵ Of these 14 transactions: six were recorded as having been reported to the staff member's Executive Director¹¹⁶; five related to newspaper subscriptions that should not have been purchased using the corporate credit card; and three were accepted.¹¹⁷
- A review of transactions from October 2021 to December 2021. The results were reported to the APRA Chief Operating Officer in December 2022. APRA documentation records that 536 transactions were reviewed, with a total value of \$175,563. Thirteen transactions, with a combined value of \$731, were identified for further investigation.¹¹⁸

2.96 APRA's compliance with credit card requirements is discussed in Chapter 4 of this audit in paragraphs 4.27 to 4.34.

Gifts, benefits and hospitality

2.97 APRA has identified risks in relation to gifts, benefits and hospitality and has established policies, procedures and arrangements to manage the identified risks.

2.98 Section 27 of the PGPA Act states that an official must not improperly use their position to gain, or seek to gain, a benefit to themselves or another person. The giving or receiving of gifts, benefits and hospitality can create the perception that an official is subject to inappropriate external influence. Perceptions of this sort can give rise to reputational risks for public entities, including the legitimacy and integrity of regulators (discussed in paragraphs 1.2 and 1.3 of this audit report).

2.99 A policy for giving and receiving gifts, benefits and hospitality is an important element of a robust control environment and supports ethical conduct. The effective implementation of such a policy, which generally requires accurate disclosures by entity personnel, benefits from strong cultural settings within the entity, including the example set by senior leadership ('tone at the top').

115 APRA advised the ANAO in January 2023 that all 'expenses were accepted by APRA with the nature of most considered reasonable. Processes have been strengthened to reduce future occurrences. This includes communication and reiteration of APRA's CFI's, processes, and review.'

116 All six transactions were for purchases of birthday cakes delivered to team members' residences.

117 APRA documentation indicates that: one purchase was for stationery while the cardholder was working from home; another was for a taxi to the office to return work equipment; and the third was for hotel accommodation that was never used as the trip was not undertaken and the room was not cancelled.

118 APRA documentation indicates the transactions were identified as they were unusual expenses, or initially not clearly consistent with corporate policies. All 13 transactions were for the purchase of birthday cakes delivered to team members' residences. APRA documentation states that APRA's Finance area's comment as 'Covid WFH [work from home] approach which has since ceased with the adoption of hybrid working'. These expenses were accepted by APRA.

2.100 APRA's policy on gifts, benefits and hospitality is contained within APRA's CFIs and applies to APRA officials.¹¹⁹ The CFIs state that:

Officials should, as a general rule, seek to avoid the receipt of gifts and offers of hospitality or sponsored travel where possible.

Officials must not accept gifts, offers of hospitality or sponsored travel, regardless of value, if the APRA official may have an actual or perceived conflict of interest as a result of receiving the gift.

2.101 The CFIs define 'the limitations and acceptable practices for Officials receiving gifts, offers of hospitality or sponsored travel from third parties' and outline:

- when it is appropriate to accept gifts, benefits and hospitality;
- declaration and approval requirements for accepting gifts, benefits and hospitality; and
- reporting requirements, including thresholds for reporting and what will be reported publicly on APRA's website.¹²⁰

2.102 APRA supplements the CFIs with intranet guidance and a document of frequently asked questions. APRA's key requirements for managing gifts, benefits and hospitality are summarised in Table 2.2.

Table 2.2: APRA's gifts, benefits and hospitality arrangements

Category	APRA requirements
Definitions of gifts, benefits and hospitality	<ul style="list-style-type: none"> • No specific definitions of gifts, benefits or hospitality but includes general descriptions in the CFIs. • APRA's intranet guidance provides specific examples of gifts, benefits and hospitality and situations when it is appropriate to accept or decline.
Approach to conflict of interest	<ul style="list-style-type: none"> • Officials must not accept gifts, offers of hospitality or sponsored travel, regardless of value, if the APRA official may have an actual or perceived conflict of interest as a result of receiving the benefit.
Declaration requirements	<ul style="list-style-type: none"> • All gifts and hospitality need to be declared in APRA's gifts register as soon as practicable (within 5 business days). • Donations offered to charity on behalf of APRA must be registered in APRA's gifts register. • Routine working lunches held on the premises of APRA-regulated entities, or external meetings over coffee, do not need to be declared as these are considered incidental and outside the scope of the policy (as the primary purpose of these is not considered to be hospitality). • Declarations are required to be entered into APRA's gifts register through APRA's online portal.

119 The CFIs define APRA officials as: 'Any person or organisation engaged by APRA to perform functions on its behalf. This includes, but is not limited to, [the] Chair, APRA Members, Staff, Contractors or Consultants'.

120 On 30 November 2021, the APSC released guidance for APS agencies (which excludes APRA) requiring agency heads to publicly disclose on their entity website, all gifts or benefits accepted valued at over \$100 (excluding GST) on a quarterly basis. The guidance states that: 'To ensure consistency and transparency across the Commonwealth, statutory office holders and heads of Commonwealth entities and companies are strongly encouraged to adopt this guidance, and mirror these arrangements, as best practice. Although not a requirement under this guidance, there is a strong expectation that agency heads will also publish gifts and benefits received by staff in their agency that exceed the threshold of \$AUD100.00 (excluding GST).' APRA has included these requirements in its policies.

Category	APRA requirements
Approval requirements	<ul style="list-style-type: none"> Minor gifts and minor hospitality can be accepted and kept by the official, up to and including a value of \$100. For gifts and hospitality valued at more than \$100, approval must be sought from the relevant APRA Member or Executive Director before acceptance (if possible). APRA Members follow the circular approval arrangements, as discussed in paragraph 2.85. Where the value is unknown, a gift or hospitality should not be regarded as minor. Approval must be sought from the relevant APRA Member or Executive Director before acceptance (if possible). Sponsored travel can only be accepted if the APRA recipient is included in an official speaking request approved by an APRA Member.
Prohibited gifts, benefits or hospitality	<ul style="list-style-type: none"> Repetitive gifts or hospitality (with a combined value of over \$100 within a six-month period).
Cultural gifts ^a	<ul style="list-style-type: none"> Non-minor gifts can be accepted, where refusal may create embarrassment or cause offence. These gifts must be handed to the relevant APRA Member, Executive Director, or APRA's Risk Management and Compliance team as soon as practicable. Non-minor offers of hospitality may be accepted, where refusal may create embarrassment or cause offence.
Requirements to surrender to APRA	<ul style="list-style-type: none"> Gifts valued at over \$100 may not be retained by the official and become the property of APRA. These gifts are to be surrendered to APRA's Risk Management and Compliance team.
Publication of gifts, benefits and hospitality registers	<ul style="list-style-type: none"> Details of gifts, hospitality and sponsored travel received over \$100 (or where the value is unknown) will be published on APRA's external website. Details of gifts, benefits and hospitality received by APRA Members are published quarterly with recipient names identified. Details of gifts, benefits and hospitality received by APRA staff are published every six months with recipient names not identified.

Note a: Cultural gifts are items of cultural or sentimental value for which a monetary value is difficult to assign.

Source: ANAO analysis of APRA documentation.

2.103 APRA's compliance with gifts, benefits and hospitality requirements is discussed in Chapter 4 of this audit in paragraphs 4.35 to 4.52.

Identification and management of fraud risks

2.104 Section 10 of the PGPA Rule requires the accountable authority to take all reasonable measures to prevent, detect and deal with fraud relating to the entity.¹²¹ It lists six requirements relating to fraud risk assessments, fraud control plans, and mechanisms for preventing fraud.

2.105 APRA's internal audit unit completed a review of fraud risk management arrangements in March 2020 (prior to the period subject to the ANAO's review). The review reported that APRA's fraud control environment and management awareness needed improvement, and made 10

121 PGPA Rule 2014 [Internet], available from <https://www.legislation.gov.au/Details/F2022C01102> [accessed 9 March 2023].

recommendations aimed at improving fraud management arrangements.¹²² During the period examined by the ANAO, APRA's internal audit team assessed the 'agreed actions' relating to these recommendations as implemented.

2.106 APRA's risk appetite statement (November 2020) states that:

APRA strives to ensure there is no fraudulent activity as part of conducting its activities. As a prudential regulator and Commonwealth entity with, in particular, access to highly confidential information, APRA has **no tolerance** for internal fraud, including instances of bribery and corruption.

There is also **no tolerance** for fraud perpetrated by external parties. APRA commits to ensuring there are internal controls in place, and working with external service providers to establish accepted practices (for example credit card fraud perpetrated on APRA business credit cards by external parties) to detect and remediate any such instances. [emphasis in original].

2.107 APRA's fraud control plan (FCP) comprises the Fraud Control Policy (September 2020) and Fraud Control Policy and Procedures 2020–2023 (September 2020). The FCP defines fraud as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means' and outlines the requirements and expectations in relation to fraud control at APRA. The FCP states that fraud 'can damage the integrity and reputation of APRA and therefore will not be tolerated within the organisation.'

2.108 APRA's FCP applies to APRA Members and staff. APRA's Executive Board approves the FCP and APRA's Audit and Risk Committee is responsible for providing assurance to the Chair on the adequacy of APRA's systems of internal control, including fraud controls.

2.109 APRA records indicate that:

- in 2020–21 there were four allegations of fraud received or detected (two internal and two external); and
- in 2021–22 there were 11 allegations of fraud received or detected (one internal and 10 external).

2.110 In both financial years the external frauds related to external charges on APRA credit cards. APRA documentation indicates that the amounts were refunded by the financial institution.

2.111 APRA's FCP sets out how APRA prevents, detects and responds to fraud and corruption risks. The ANAO assessed whether APRA's FCP and arrangements complied with section 10 of the PGPA Rule. Overall, as outlined in Table 2.3, APRA has met the requirements of section 10.

122 The report identified that: APRA's Fraud Control Policy and procedures document complied with key compliance obligations, but the policy had not been effectively embedded across APRA; risk assessments did not assist in understanding and assessing APRA's fraud risks; not all staff had received fraud awareness training in the previous 12 months; and mitigating controls were ineffective.

Table 2.3: Fraud control requirements and APRA compliance

PGPA Rule section 10 requirement	Meets requirement	Description/examples of APRA arrangements
Conduct a fraud risk assessment regularly and when there is a substantial change in the structure, functions or activities of the entity.	✓	Business units identify fraud and corruption risks and record them in APRA's divisional risk registers which are reviewed six monthly. Enterprise Risks are reported to the Audit and Risk Committee, Executive Committee and Executive Board. ^a
Develop and implement a fraud control plan that deals with identified risks as soon as practicable after conducting a risk assessment.	✓	APRA has a fraud control plan (FCP) in place.
Have an appropriate mechanism for preventing fraud, including by ensuring that: (i) officials of the entity are made aware of what constitutes fraud; and (ii) the risk of fraud is taken into account in planning and conducting the activities of the entity.	✓	APRA staff are required to complete training upon commencement and refresh annually. APRA advised the ANAO that the completion of training is monitored by General Managers across the organisation although results are not formally reported to senior management. Training materials include defining fraud. APRA's intranet includes information relating to fraud including how to report suspected or actual fraud or corruption. There is regular risk and governance reporting on divisional risk landscapes to the Executive Board. Annually the Audit and Risk Committee is provided with an update on fraud control activity during the year. Feedback from the Audit and Risk Committee is considered when conducting entity activities and reporting.
Have an appropriate mechanism for detecting incidents of fraud or suspected fraud, including a process for officials of the entity and other persons to report suspected fraud confidentially.	✓	APRA's CFIs require staff to report incidents of suspected or potential fraud in accordance with the FCP. Fraud can be reported by various means, including anonymously, and staff can report suspected fraud, bribery or corruption to the Commonwealth Ombudsman. APRA can also receive reports of alleged fraud from internal and external audits and reviews, members of the public, external contractors, service providers and other Government agencies, including law enforcement bodies.
Have an appropriate mechanism for investigating or otherwise dealing with incidents of fraud or suspected fraud.	✓	APRA's FCP sets out mechanisms for investigating and dealing with fraud or suspected fraud incidents. The Chief Risk Officer (guided by APRA's Executive Board, where necessary) is responsible for the final decision on whether a formal investigation will be conducted internally by APRA or externally.

PGPA Rule section 10 requirement	Meets requirement	Description/examples of APRA arrangements
Have an appropriate mechanism for recording and reporting incidents of fraud or suspected fraud.	✓	<p>APRA officials must report suspected or actual instances of fraud to APRA's Fraud Control Officer, their line manager, General Manager, Executive Director or the Chief Risk Officer.</p> <p>The Chief Risk Officer is required to report instances of fraud to APRA's Executive Board and the Executive Board must be notified of all fraud investigations.</p> <p>Any allegations of fraud committed by the APRA Chair must be reported to the Chief Risk Officer. Any allegations of fraud committed by the Fraud Control Officer must be reported to the Chief Risk Officer.</p>

Note a The Audit and Risk Committee receives updates on risk management, which includes fraud, at each quarterly meeting. The Executive Committee receives monthly updates (at every second meeting) from the Chief Risk Officer, including on fraud. The Executive Board receives Minutes from both the Audit and Risk Committee and the Executive Committee, in addition to receiving updates from the Chief Risk Officer, which includes fraud, at most monthly meetings.

Source: ANAO analysis of APRA documentation.

Public interest disclosures

2.112 APRA has established a public interest disclosure (PID) policy that is accessible to both APRA officials and the public; has identified authorised officers; has training relating to PID available to APRA officials and provides PID guidance on its intranet and website.

2.113 The *Public Interest Disclosure Act 2013* (PID Act) establishes a PID scheme where public officials 'who suspect wrongdoing within the Commonwealth public sector can raise their concerns.'¹²³ The PID Act 'applies to Australian Government agencies, Commonwealth companies, public authorities and Commonwealth contracted service providers.'¹²⁴ The purpose of the PID Act is to:

promote the integrity and accountability of the Commonwealth public sector by:

- encouraging and facilitating the making of disclosures of wrongdoing by public officials
- ensuring that public officials who make protected disclosures are supported and protected from adverse consequences relating to the making of a disclosure

123 Commonwealth Ombudsman, *Public interest disclosure (whistleblowing)* [Internet], Commonwealth Ombudsman, available from <https://www.ombudsman.gov.au/complaints/public-interest-disclosure-whistleblowing> [accessed 7 March 2023].

A person "must be a current or former 'public official' as defined in section 69 of the PID Act, to make a public interest disclosure ... Individuals and organisations that provide goods or services under a Commonwealth contract ... and their officers or employees are also public officials for the purposes of the PID Act."

Commonwealth Ombudsman, *Agency Guide To The Public Interest Disclosure Act 2013 Version 2* [Internet], Commonwealth Ombudsman, April 2016, p. 4, available from https://www.ombudsman.gov.au/_data/assets/pdf_file/0020/37415/Agency_Guide_to_the_PID_Act_Version_2.pdf [accessed 7 March 2023].

124 Commonwealth Ombudsman, *Information for Agencies* [Internet], Commonwealth Ombudsman, available from <https://www.ombudsman.gov.au/industry-and-agency-oversight/public-interest-disclosure-whistleblowing/information-for-agencies> [accessed 7 March 2023].

- ensuring that disclosures are properly investigated and dealt with.¹²⁵

2.114 The kinds of conduct that disclosures can be made about include but are not limited to:

- a contravention of the law
- corruption
- perverting the course of justice
- maladministration
- an abuse of public trust
- falsifying scientific research
- wastage of public money, or
- conduct that is a danger to health, safety or the environment.¹²⁶

2.115 The PID Act sets out a range of obligations including those relating to the principal officer of each agency¹²⁷ and authorised officers.¹²⁸

2.116 The ANAO examined whether APRA had:

- established a PID policy that is accessible to APRA officials and the public;
- identified authorised officers;

125 Commonwealth Ombudsman, *Agency Guide To The Public Interest Disclosure Act 2013 Version 2* [Internet], Commonwealth Ombudsman, April 2016, p. 2, available from https://www.ombudsman.gov.au/data/assets/pdf_file/0020/37415/Agency_Guide_to_the_PID_Act_Version_2.pdf [accessed 7 March 2023].

126 Commonwealth Ombudsman, *Public interest disclosure (whistleblowing)* [Internet], Commonwealth Ombudsman, available from <https://www.ombudsman.gov.au/complaints/public-interest-disclosure-whistleblowing> [accessed 7 March 2023].

127 A principal officer is the head of an agency or their delegate. In APRA, the APRA Chair is the principal officer. The PID Act requires a principal officer to:

- Appoint a sufficient number of authorised officers to receive internal PIDs in your agency
- Ensure the authorised officers are accessible to current and former public officials of your agency
- Establish written PID procedures for your agency and ensure these are accessible
- Broadly promote the PID scheme to public officials as an effective way to speak up about wrongdoing
- Promptly act to investigate and address allegations of wrongdoing
- Delegate powers and responsibilities as are necessary for the effective operation of the PID scheme
- Influence an organisational culture that supports public officials who speak up about wrongdoing and does not tolerate reprisal against them
- Drive change to address problems uncovered through the investigation of internal PIDs.

Commonwealth Ombudsman, *Public Interest Disclosure Scheme Reference Guide* [Internet], Commonwealth Ombudsman, p. 1, available from https://www.ombudsman.gov.au/data/assets/pdf_file/0024/37428/pid_reference_guide.pdf [accessed 7 March 2023].

128 An ‘authorised officer is a public official who belongs to the agency and is either the principal officer or is appointed in writing as such by the principal officer.’

Commonwealth Ombudsman, *Agency Guide To The Public Interest Disclosure Act 2013 Version 2* [Internet], Commonwealth Ombudsman, April 2016, p. 16, available from https://www.ombudsman.gov.au/data/assets/pdf_file/0020/37415/Agency_Guide_to_the_PID_Act_Version_2.pdf [accessed 7 March 2023].

Amongst other things, authorised officers provide advice to public officials about PIDs and assess whether allegations of wrongdoing constitute a PID.

- PID training available for staff; and
- provided PID related guidance on its intranet and website.

2.117 APRA has a public interest disclosure policy. The policy is available on APRA's intranet and website so is accessible to both APRA officials and the public. This policy includes information on:

- what is a public interest disclosure;
- what is disclosable conduct;
- who can make a public interest disclosure;
- protections under the PID Act;
- how to make a public interest disclosure;
- roles and responsibilities;
- what happens after a public interest disclosure is made;
- confidentiality requirements; and
- support arrangements.

2.118 A public interest disclosure can be made by current and former public officials including APRA current or former staff (including temporary and contracted employees), APRA Members and service providers contracted to APRA (including their officers and employees). APRA's policy states that:

An authorised officer of an agency may also deem a person to be a public official if they believe on reasonable grounds that the person has information that concerns disclosable conduct, the person has disclosed or proposes to disclose the information to the authorised officer, and the person was not a public official when they obtained the relevant information. Such a determination may be made by the authorised officer of an agency upon receipt of a request from the relevant person, or by the authorised officer on their own initiative.

2.119 APRA also provides guidance relating to public interest disclosure on its intranet. APRA's website includes a link to its PID policy and the email address to be used to make a disclosure to an authorised officer.

2.120 As of 24 March 2023, APRA had 14 authorised officers. APRA also has mandatory training related to PID as part of the annual refresher course for staff (see Table 2.4 for details). There is no additional training related to PID for authorised officers.

Were relevant policies subject to periodic review?

APRA has established a framework for the design and review of its policies. For the selected probity risks, there was evidence of relevant policies being reviewed and updated.

2.121 Periodic review of entity policies assists in ensuring they remain fit-for-purpose and address current risks. For the period examined as part of this audit, the ANAO examined whether relevant policies were subject to periodic review.¹²⁹

¹²⁹ Relevant policies are those related to the probity risks outlined in the audit scope section of Chapter 1 of this audit (see paragraph 1.25).

2.122 APRA has established 'Enterprise Policy Principles' (March 2020) that 'formalise and outline APRA's approach to the management and review of enterprise-wide policy documents.'¹³⁰ As part of these arrangements, APRA maintains a policy register which includes a list of all current policies, the policy owner, the last approval date and the next date of review.¹³¹ The policy owner is responsible for maintaining the policy, including the content, approval of minor updates and publishing the policy on the Enterprise Policy Register — APRA's central location for all enterprise policies and procedures.

2.123 Over the period examined for this audit, relevant APRA policies were reviewed and updated.¹³²

Does APRA effectively inform its personnel of probity requirements and promote compliance?

For the selected probity risks, APRA has effectively informed its personnel of probity requirements. APRA has adopted a combination of training, making information on policies, procedures and arrangements easily accessible on its intranet, and messaging from senior officials to reinforce knowledge of probity requirements and promote compliance. APRA tracks the completion of annual refresher training and reports the results to senior management.

2.124 The effectiveness of an entity's arrangements for managing probity risks is dependent on personnel being effectively informed of the requirements with which they are required to comply. This can be done through, for example:

- the provision of training;
- making information on policies, procedures and arrangements addressing probity risks easily accessible to staff; and
- regular messaging from senior officers.

Training related to probity risks

2.125 APRA has a suite of training, some of which is mandatory, that addresses the probity risks examined in this audit. APRA has training that staff and Members must complete within either one or three months of commencement.¹³³ Permanent APRA employees must also complete a six-hour induction course within their first three months.¹³⁴ APRA advised the ANAO in January 2023 that 'Members who are new to the organisation are encouraged but not required to attend' the six-hour

130 The Enterprise Policy Principles apply to all policies and procedures which cover enterprise-wide internal governance matters such as financial management, risk management, people management and security and information management.

131 APRA advised the ANAO in January 2023 that the Enterprise Policy Register site was created on 6 February 2020.

132 See Appendix 2 of this audit report for examples of policies updated during the period covered by this audit.

133 Training required to be completed within the first month of commencing relates to: discrimination, inclusion and diversity; workplace health and safety awareness; security; 'keeping on the right side of the law'; and fraud awareness. Training required to be completed within three months of commencement relates to enterprise risk management; business continuity; and using APRA's information management system.

134 APRA advised the ANAO in January 2023 that the induction course includes: introduction to APRA's history, role and values; prudential regulation; risk management and compliance; security; people and culture; inclusion and diversity; social club and wellbeing and resilience.

induction course. APRA further advised that Members are also provided with a detailed onboarding pack and the Chair is provided an additional document outlining key legislative responsibilities of the Chair's role.

2.126 Staff are required to complete an annual compliance refresher that covers key elements of the initial suite of training. Contingent workers who have been at APRA for longer than one year are also required to complete the annual refresher training.¹³⁵

2.127 APRA staff involved in prudential supervision are invited to undertake additional supervision training.¹³⁶ Table 2.4 provides details of the training available for the probity risks examined in this audit.

Table 2.4: APRA probity related training

Probity risk	Mandatory training available	Frequency of required renewal
Code of conduct	Yes Included in introductory modules.	Not required
Conflict of interest	Yes Included in introductory modules and annual refresher.	Annually
Regulatory capture	No	Not required
Financial holdings disclosure	Yes Included in introductory modules.	Not required
Confidentiality and information security	Yes Included in introductory modules and annual refresher.	Annually
Procurement	No ^a	Not required
Corporate credit card expenditure	No ^b	Not required
Gifts, benefits and hospitality	Yes Included in introductory modules and annual refresher.	Annually
Fraud	Yes Included in introductory modules and annual refresher.	Annually

¹³⁵ APRA advised the ANAO that:

Contingent workers are defined as workers that provide services to APRA, but are not on the organisation's payroll and do not get paid entitlements (i.e. personal leave). Their engagement is temporary to undertake a specific task or project for an agreed tenure and rate of pay.

Contingent workers generally include: contractors (that perform activities akin to a staff member for a specified duration), consultants (that provide a specific deliverable or advice), contracted services and work experience.

¹³⁶ Roles involving prudential supervision are in the banking, insurance and superannuation divisions.

Probity risk	Mandatory training available	Frequency of required renewal
Public interest disclosures	Yes Included in introductory modules and annual refresher.	Annually

Note a: For procurements over \$20,000, APRA staff must work with the procurement team. APRA advised the ANAO that the procurement team has specialist training to manage procurement.

Note b: APRA advised the ANAO that while there is no training on how to use a credit card, cardholders must agree to specified terms and conditions as part of the application process for obtaining a card.

Source: ANAO analysis of APRA documentation.

2.128 APRA advised the ANAO in January 2023 that it tracks the completion of the probationary one month and three month training:

Business Unit managers in each division also oversee new hire completion of mandatory training.

The PeopleHub system also sends automated reminders to employees when mandatory training has been assigned, 7 days prior to due date and 7 days past due date.

2.129 APRA tracks the completion of annual refresher training and reports on completion rates to the Executive committee. The due date for the most recent annual refresher training cycle conducted during this audit was 10 February 2023. The completion rate as at 3 February 2023 (74.6 per cent) was provided to business managers for each division, APRA's internal audit area, and APRA's executive office. APRA documentation reported a completion rate of 97.2 per cent as at the due date of 10 February 2023. This was reported to the Executive Committee on 21 February 2023.

Accessibility of information on probity requirements

2.130 APRA makes policies, procedures and information regarding arrangements to address probity risks available on its intranet. Often this information contained contact details for specialist staff who can provide assistance.

Messaging from senior officials

2.131 APRA uses a range of channels for providing its personnel with information on probity requirements, including information on policy updates, reminders regarding obligations and senior officials' expectations. These channels include:

- APRA news and the Voice of APRA¹³⁷;
- awareness campaigns — for example targeted reminders at the end of the financial year and calendar year in relation to gifts, benefits and hospitality — to raise awareness of requirements; and
- email reminders to all staff.

¹³⁷ APRA news is an internal bulletin that includes information and updates for APRA staff. The Voice of APRA is an internal communication from APRA Members that provides general updates and information to APRA staff. Contractors with system access will receive the same communication as APRA staff, including APRA news and the Voice of APRA.

3. Monitoring, reporting and assurance

Areas examined

This chapter examines whether the Australian Prudential Regulation Authority (APRA) has established monitoring and reporting arrangements to provide assurance on the effectiveness of its internal controls and compliance with probity requirements, and arrangements to follow up on identified instances of non-compliance. The period examined in this audit was July 2020 – November 2022 and where relevant, included key subsequent events up to and including February 2023.

Conclusion

APRA has a framework and arrangements for monitoring the effectiveness of internal controls and compliance with probity requirements, and for providing assurance to the accountable authority in relation to probity. The framework includes regular compliance monitoring, reporting to management and high-level governance committees, and arrangements for following up on identified instances of non-compliance. Key activities are overseen by a Risk Management and Compliance team.

3.1 An entity's accountable authority is required to establish appropriate controls and maintain sufficient oversight to ensure internal controls operate as intended, to assist in mitigating probity related risks and promote compliance. Well-functioning assurance arrangements, including reporting to senior management, provide confidence that risks are being effectively controlled or identify when controls are ineffective or absent. Entities also need to ensure that instances of non-compliance are treated in a timely and appropriate manner in accordance with specified requirements.

3.2 This chapter examines whether APRA has established monitoring and reporting arrangements to provide assurance on the effectiveness of internal controls and compliance with probity requirements. Specifically, the ANAO examined if APRA has established a fit for purpose framework for:

- monitoring the effectiveness of internal controls relating to probity and providing assurance to the accountable authority;
- monitoring compliance with probity requirements, including regular monitoring and reporting; and
- following up on identified instances of non-compliance.

Is there a framework for monitoring the effectiveness of internal controls relating to probity and providing assurance to the accountable authority?

APRA has a framework for monitoring the effectiveness of internal controls and providing assurance to the accountable authority in relation to probity. The framework includes regular internal audits into probity related topics and periodic assessment of control effectiveness. Reporting on internal audits and the effectiveness of internal controls is provided to the

Executive Board, Executive Committee and the Audit and Risk Committee. The accountable authority is a member of the Executive Board and Executive Committee.

3.3 Information on the effectiveness of internal controls gives the accountable authority assurance regarding compliance with probity policies and the extent to which staff uphold standards of conduct. Section 16 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires the accountable authority of a Commonwealth entity to establish an appropriate system of internal control. Section 17 of the Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) requires the accountable authority to establish an audit committee, the functions of which must include reviewing the appropriateness of the system of internal control. This would include coverage of oversight of the management of identified probity risks.

Internal audit

Review activity

3.4 APRA undertakes internal audits (which provide ratings of 'sound', 'satisfactory', 'unsatisfactory' or 'needs improvement') and advisory reviews (which do not provide ratings).¹³⁸ In developing its internal audit plan, APRA considers factors such as key areas of risk, thematic risk changes from the previous year, and previous audits that have provided ratings of 'needs improvement'.

3.5 During the period examined in this audit, APRA conducted the following internal audits that related to the probity risks examined by the ANAO.

- Bi-Annual review of Members' credit card transactions (both of which provided ratings of 'satisfactory' and were discussed in paragraph 2.92).
- Whistleblower/conflict of interest (which provided a rating of 'needs improvement').¹³⁹
- Procure to pay end to end (which provided a rating of 'needs improvement' and was discussed in paragraph 2.67).
- Expense management (which provided a rating of 'needs improvement').¹⁴⁰

3.6 APRA advised the ANAO that for audits which provided ratings of 'needs improvement' or 'unsatisfactory', the protocol is to examine the topic again within 12 to 18 months.

138 In 2020–21 APRA completed 11 internal audits and six advisory reviews. APRA advised the ANAO in January 2023 that nine internal audits and seven advisory reviews were completed in 2021–22. APRA documents state that advisory reviews are typically conducted: when a timely independent opinion is required without the need to test the full spectrum of controls testing; where an independent opinion (not focussed on control activities) is required; and where early guidance from a risk and controls perspective is required to inform management action. APRA advised the ANAO that:

Historically ... advisory reviews were not provided with a rating ... moving forward advisory reviews are now provided with an overall rating. Hence, despite a review having an attached rating ... it could still be an advisory engagement by nature.

139 The audit scope was reported as 'focused on assessing the alignment of APRA's WB [whistleblowing] and COI [conflict of interest] policies with compliance obligations, and whether supporting procedures and practices are adequately understood and embedded.' For sample testing purposes, the audit covered the period 1 July 2019 to 31 August 2021.

140 This internal audit reported on credit cards and employee expense vouchers for the period 1 January 2019 to 31 January 2021.

3.7 APRA also conducted one advisory review relating to probity in 2020–21 — the Probity Advisory Review completed in October 2020.¹⁴¹ The review stated that:

Overall, while expected probity practices are in place, regular monitoring and reporting practices need to be enhanced to appropriately demonstrate that APRA's probity controls are operating effectively. Supporting documentation can also be improved to explicitly outline key expectations, and training and communication need to be enhanced to elevate awareness. As an advisory review, an overall rating was not provided. However, observations and actions from this audit should be used to elevate APRA's practices across its probity management activities.¹⁴²

3.8 Observations from the Probity Advisory Review were combined with insights gained from engagement with the Australian Securities and Investments Commission (ASIC) and recommendations from the Thom review of ASIC's governance arrangements, to create a list of 'probity actions'. The probity actions included improvements to:

- training and general awareness of probity requirements;
- assurance arrangements and review processes;
- arrangements for statutory appointees, including relocation and expenses management;
- central reporting of breaches; and
- probity related policies and procedures.

3.9 APRA's Audit and Risk Committee was advised in August 2021 that all the actions had been implemented, except for two which related to upcoming internal audits.¹⁴³

Oversight

3.10 Under its Charter, the role of Audit and Risk Committee is to 'provide independent advice to the APRA Chair on APRA's financial and performance reporting responsibilities, risk oversight and

141 APRA documentation stated that:

The review will examine the design and adequacy of APRA's probity controls in ensuring:

- Roles, responsibilities, and accountabilities are clearly defined.
- Policies and procedures fully reflect legislative requirements, are regularly reviewed, and activities have been embedded into business processes to ensure they are consistently adhered to.
- Relevant governance committees receive periodic reporting on compliance with probity requirements to ensure visibility of probity management within APRA.
- Effective protocols are in place to ensure incidents of non-compliance are reported, investigated, and addressed in a timely manner.
- Formal training programs, communication, and guidance materials are in place to raise staff awareness of probity requirements.

142 The report from the review included three observations: address gaps in training, awareness and communication to support increased user compliance; increase assurance and visibility of compliance and management of Conflicts of Interest; and improve the process for review and approval of Members' credit card transactions. The report also included two improvement opportunities. The first related to updating APRA's procurement intranet page and the second related to providing more explicit guidance in relation to cost centre managers' review of credit card transactions. The report also listed what actions would be undertaken to 'remediate the weaknesses highlighted'. APRA documentation indicates that actions arising from the three observations were all completed by 14 December 2021.

143 The internal audits related to expense management (completed in October 2021) and procurement (completed in January 2022).

management, and system of internal control.’ The Audit and Risk Committee receives updates on APRA’s internal control framework.

3.11 Internal audit reports are discussed as a standing agenda item at the Audit and Risk Committee and APRA Executive Board meetings.¹⁴⁴ APRA advised the ANAO in January 2023 that audit reports rated as ‘needs improvement’ and ‘unsatisfactory’ are submitted to the Audit and Risk Committee and Executive Board.¹⁴⁵ The Executive Committee¹⁴⁶ also receives updates on open audit action items monthly, at every second meeting.

3.12 APRA has reviewed aspects of its oversight arrangements relating to the internal control environment. Documentation provided to APRA’s Audit and Risk Committee in October 2021 observed that:

under current reporting protocols, there is limited visibility of Management oversight and actions to address any significant observations impacting the control environment. Reliance was placed solely on Management to carry out its accountability. Without sufficient visibility, it was difficult for the ARC [Audit and Risk Committee] to form an opinion on whether significant control gaps were identified and what remediation actions were agreed. In addition, Advisory Review actions are not captured in ERICA [APRA’s Enterprise Risk, Information, Compliance and Accountability management system], leading to the potential for relevant remediation actions to not be implemented in a timely manner ... based on current protocols, material recommendations had the potential to be interpreted as actions to be done on a best endeavour basis, rather than actions that Management must undertake.

3.13 APRA documentation indicates that to address these issues and to identify potential enhancements, Internal Audit revised its approach to advisory reviews. The effect of this was that any observation stemming from an advisory review in the category of governance, strategy, risk appetite, security or compliance would be risk rated as per standard internal audit observations, with agreed actions to be captured and tracked in ERICA.¹⁴⁷ A summary of non-rated observations arising from advisory reviews would be presented to the Audit and Risk Committee as part of the internal audit quarterly update, in addition to the full report.

144 The Executive Board (Risk) also received internal audit updates until its final meeting on 15 November 2021. The Executive Board (Risk) was discontinued and merged into the Executive Board. The Executive Board (Risk) meetings operated under the Executive Board Charter and were considered to be a ‘focused’ meeting of the Executive Board rather than a separate committee.

145 APRA advised the ANAO in January 2023 that: a summary of key themes for other reviews is provided in the Quarterly Internal Audit Report to both committees.

146 The Executive Board is comprised of all APRA Members and the Executive Committee is comprised of the APRA Members and APRA Executive Directors. APRA advised the ANAO in January 2023 that from December 2022, Internal Audit provides a monthly dashboard to the Executive Committee with a quarterly thematic report which includes more detail on execution of plan and outcomes from Internal Audit reports. APRA further advised that all APRA Members and other Executive Committee members receive a copy of all final Internal Audit reports.

147 As noted in paragraph 3.12, ERICA is APRA’s Enterprise Risk, Information, Compliance and Accountability management system.

Internal assessment of the effectiveness of controls

3.14 APRA's Compliance Management Policy 2022 (compliance policy) sets out APRA's policy for managing compliance.¹⁴⁸ In respect to internal controls¹⁴⁹, the compliance policy states that:

Identifying controls and reviewing their effectiveness are fundamental elements of the risk and compliance assessment process ... Each Business Unit owns and maintains its controls within ERICA. Part of the overall compliance obligation assessment approach involves assessing the effectiveness of controls (i.e. whether they are effective, partially effective or ineffective).

3.15 The Executive Committee and Audit and Risk Committee receive reports, twice a year, on the results of assessments of the effectiveness of internal controls relating to various compliance obligations. Controls assessed through this process include those relating to:

- compliance with the PGPA Act;
- compliance with the *Australian Prudential Regulation Authority Act 1998* (APRA Act)¹⁵⁰;
- compliance breaches;
- code of conduct;
- conflict of interest;
- procurement; and
- gifts and hospitality.

3.16 In June 2022, APRA reported that in its most recent assessment process, out of a total of 437 compliance obligations, controls relating to:

- 298 obligations (66.1 per cent) were assessed as effective;
- 139 obligations (33.9 per cent) were assessed as partially effective; and
- none were assessed as not effective.

3.17 In addition to this overall (entity-level) assessment of the effectiveness of the control environment, a comparative (by division) and historical analysis was also provided to the Executive Committee and the Audit and Risk Committee.¹⁵¹

148 APRA's compliance management framework is discussed further in paragraphs 3.18 to 3.26.

149 The compliance policy defines controls as any activity, tool, management process or document that modifies the rating of the risk (for example, in this instance, compliance risk). For example, a control, if operating as intended, is expected to either reduce the likelihood of a risk occurring or limit its impact should the risk materialise.

150 For example, section 48AB of the APRA Act establishes a requirement for the determination of APRA Values and section 48AC establishes a requirement for the Chair to determine the APRA Code of Conduct. Both of these requirements are listed in the Obligation Register and are reviewed periodically.

151 It was reported that: 'There has been a decrease in the overall effectiveness of controls from 86.6% to 66.1%. Given the focus on uplifting controls across APRA and greater scrutiny, particularly in PAD [Policy and Advice Division] and Insurance, the results of 33.9% Partially Effective is not unexpected. Insurance account for 92 of the 139 partially effective control assessments ... RMC [Risk Management and Compliance] has been monitoring work on the uplift of controls and assesses the deficiencies as being known, actions are in place and work to remediate is ongoing.'

Is there a framework for monitoring compliance with probity requirements, including regular monitoring and reporting?

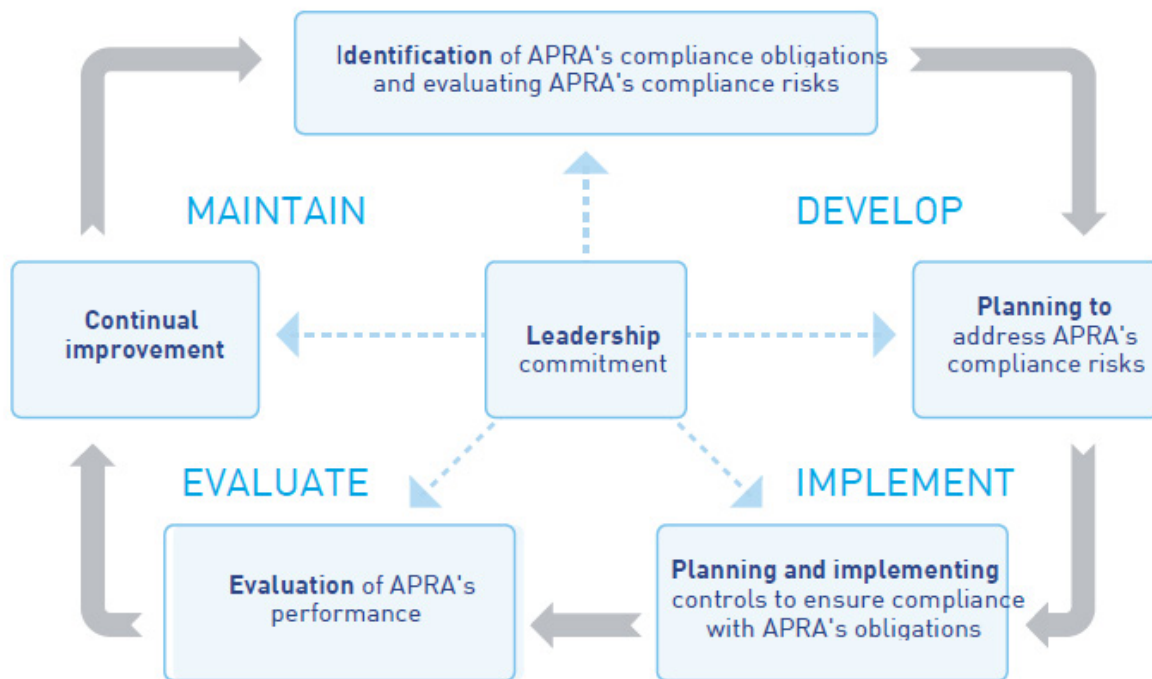
APRA undertakes regular compliance monitoring under its compliance management framework, and has established a Risk Management and Compliance team which reports on a regular basis to the Audit and Risk Committee and the Executive Committee on compliance with obligations, including obligations related to probity requirements. APRA's compliance management framework includes a register of compliance obligations, and Reportable Incident and Escalation Standards which establish reporting obligations.

Compliance policy

3.18 APRA's Compliance Management Policy document outlines APRA's compliance management framework, which comprises the following:

- a register of external compliance obligations;
- incident reporting and escalation standards;
- conflicts of interest framework (including for gifts and hospitality);
- compliance monitoring;
- compliance training;
- compliance reporting and management oversight;
- actions management;
- controls management; and
- consequence management.

The intended operation of APRA's compliance management framework is illustrated in Figure 3.1.

Figure 3.1: Flowchart of APRA's Compliance Management Framework

Source: APRA Compliance Management Policy.

Compliance Obligation Register

3.19 Central to APRA's compliance framework is the Compliance Obligation Register (register). The register is stored in ERICA and contains all external obligations applicable to APRA.¹⁵² Some obligations apply entity-wide while others only apply to certain areas within APRA.

3.20 APRA's Compliance Management Policy requires obligations to be reviewed at least quarterly by the Risk Management and Compliance Division. Obligation owners are assigned to each compliance obligation in the register and are periodically required to complete a compliance assessment for the obligations assigned to them. The frequency of this review is determined by the obligation's risk rating. Obligations with a 'high' risk rating are reviewed every six months, 'medium' rated obligations are reviewed annually, and 'low' rated obligations are reviewed every two years. The compliance assessment includes the evaluation of the effectiveness of controls in relation to each obligation (discussed in paragraphs 3.14 and 3.15).

3.21 In June 2022 the results of the then most recent 'high' and 'medium' rated compliance obligation assessments were reported to the Executive Committee and the Audit and Risk Committee.¹⁵³ This included an assessment of 437 obligations, some of which related to

¹⁵² External obligations include legislative requirements that APRA is required to comply with or has regulatory responsibility for.

¹⁵³ The assessment of APRA's high and medium rated compliance obligations was conducted between 15 March 2022 – 15 April 2022.

probity.¹⁵⁴ Where non-compliance was found, specific information was provided about the division affected, the relevant obligation, and its risk rating.¹⁵⁵ No non-compliance was found in respect to obligations relating to probity.

3.22 An obligations assessment was also conducted in 2021, covering 'high', 'medium' and 'low' rated obligations. A total of 768 obligations was assessed.¹⁵⁶

Reportable Incident and Escalation Standards

3.23 The compliance policy also outlines requirements for incident reporting and the escalation and analysis of issues.

3.24 The requirements are set out in APRA's Reportable Incident and Escalation Standards, which outline minimum standards and expectations for the timely identification, management, monitoring and escalation of reportable incidents and near misses.¹⁵⁷ The Standards provide guidance on:

- responsibilities¹⁵⁸;
- incident reporting;
- impact assessment and subsequent reporting;
- escalation;
- analysis; and
- reporting to the Audit and Risk Committee and the Executive Committee on reportable incidents.

3.25 Incidents logged in ERICA¹⁵⁹ are reported to the Risk Management and Compliance team.¹⁶⁰ Details of reportable incidents are provided to the Audit and Risk Committee and the Executive

154 Probity related obligations included the following:

- The Chair must determine, in writing, the APRA Code of Conduct.
- The organisation should maintain a central register to record gifts, hospitality, travel as well as political and charitable donations.
- Officials of the NCE [non-corporate Commonwealth entity] must report material personal interests that relate to the affairs of the entity they work for.

155 Summary data was provided. The number of 'compliant' obligations was reported as 434, and the number of 'non-compliant' obligations was reported as three.

156 Summary data was provided. The number of 'compliant' obligations was reported as 766, and number of 'non-compliant' obligations was reported as two.

157 The Standards define a reportable incident as 'an event (manifestation of a risk) that has, or could have (a near miss), a negative consequence (either financial or non-financial) for APRA. They are a failure to comply with a specific area of legislation, or a breakdown in, or absence of, internal controls required to support adequate and ongoing management of APRA's operations. Consequences can be potential, actual or perceived. Reportable incidents must be reported to ERICA.'

158 The Standards provide that Executive Directors and Divisional Risk Leads can obtain information such as incident reporting for their Divisions, to get an overview of any trends and the status of rectification actions, in order to support their role in the incident management process.

159 Incidents relating to workplace health and safety, technical/IT, phishing/email scams, concerns regarding workplace behaviour and employment disputes, public interest disclosure, fraud, building services/facilities, privacy, and whistleblowing, are reported through other channels. All other incidents, such as operational risk incidents, are reported through ERICA.

160 This team is responsible for compliance monitoring and assurance, in addition to maintaining APRA's conflict of interest and gift registers.

Committee. Reporting to the Executive Committee includes the total open actions arising from incidents, the number of overdue actions, and how many actions are due in 90 days.

3.26 The Compliance Policy states that:

Each Division is responsible for ensuring their employees are aware of their requirements to log reportable incidents and escalate these to management (i.e. immediate manager and/or senior management) where required, in accordance with APRA's Reportable Incident and Escalation Standards. All reportable incidents are to be logged in the Incidents Register in ERICA as outlined in the Reportable Incident and Escalation Standards. Where an incident has been raised, and where possible, any relevant Compliance Obligation should be noted in the incident documentation. Furthermore in obligation assessments, where an obligation is assessed as 'not compliant', an incident should be created.

Other reporting on compliance with probity requirements

3.27 As discussed, APRA's Executive Board receives a variety of reporting on compliance with probity requirements. This also includes reporting on:

- training and awareness activities¹⁶¹;
- code of conduct¹⁶²;
- conflict of interest declarations¹⁶³; and
- APRA's gift register.¹⁶⁴

3.28 APRA also reports to the Audit and Risk Committee each quarter on key metrics relating to compliance with various probity related policy requirements. This includes reporting based on attestations made by senior executives relating to:

- conflict of interest declarations;
- compliance breaches;
- financial holdings disclosures;
- incidents reported; and
- APRA's Risk Appetite dashboard.¹⁶⁵

161 This includes completion rates of the mandatory annual refresher training.

162 This includes reporting of activities related to code of conduct, including: incident reporting of misuse of credit cards; inappropriate access to documents; compliance breaches such as information breaches; fraud; and staff grievances reported and under ongoing investigation.

163 This includes reporting on any new breaches related to conflict of interest and outlines if there are any historical breaches that are being investigated. Updates of the annual declaration process are also reported.

164 This includes reporting on gifts recorded in the gift register, with details of staff members who received the gift, who the gift was received from, the gift's description and value.

165 APRA's Risk Appetite dashboard consists of 16 risk statements that are aligned with APRA's six key organisational pillars of: policy; supervision; resolution; risk intelligence and frameworks; people and culture; and organisational effectiveness. On a quarterly basis, the Risk Owners of these 16 risk statements provide their perspective on whether their risks are within or outside of appetite, and what the outlook is for the following period.

Is there a framework for following up on identified instances of non-compliance?

APRA has a framework for following up on identified instances of non-compliance. The framework is documented in APRA's Compliance Management Policy, which is supported by Reportable Incident and Escalation Standards and related guidance.

3.29 Having a framework for following up on identified instances of non-compliance assists in providing assurance to the accountable authority regarding the effectiveness of probity management arrangements.

Responding to non-compliance with probity requirements

3.30 APRA's compliance management policy provides that all APRA managers, employees, contractors and suppliers are responsible for reporting incidents of non-compliance. Managers have additional responsibilities to report incidents of non-compliance that are reported to them, respond to deficiencies in controls and ensure that employees, contractors, and suppliers they manage have a clear understanding of their compliance responsibilities and accountabilities specific to their role.

3.31 Divisions maintain their own controls in ERICA and where controls are assessed to be ineffective or partially effective, the relevant Division has responsibility for determining whether it creates a mitigation or improvement action/plan. APRA's compliance management policy states that:

Where there is a need to mitigate a risk or correct a control deficiency (including remediation of non-compliance with an obligation, or remediation of a partial or ineffective control linked to an obligation), the relevant Division is to identify, record, undertake and monitor timely completion of an Action.

3.32 The Risk Management and Compliance team has responsibility for oversight of this process and for presenting information to the Audit and Risk Committee and Executive Board regarding the status of compliance obligations.

Consequences for non-compliance with probity requirements

General approach

3.33 APRA's compliance management policy states that:

Non-compliance with this Policy could have a serious impact (e.g. a breach of a legislative requirement) and reputational damage for APRA. All employees are responsible for understanding how compliance obligations apply to their role.

Disciplinary action may apply depending on the severity (including the potential impact) of a failure to comply with an obligation.

3.34 As discussed in paragraphs 3.23 to 3.26, APRA's compliance management policy provides that instances of non-compliance must be reported pursuant to the Reportable Incidents and Escalation Standards. These standards provide that, based on the type of incident and if it is deemed to be reportable, it may also be recorded by the process owner in ERICA.

3.35 APRA has a Consequence Management Framework which outlines the approach to be applied to all employee performance and conduct management and provides examples of employee performance and conduct issues with possible interventions and consequences. The framework also indicates that the severity of consequences depends on both the severity of risk and impact, and the severity of misconduct. APRA advised the ANAO that:

it was agreed that this [Consequence Management Framework] should not be viewed as a policy document or formal framework, but an informal guide for EDs [Executive Directors], Members, P&C [People and Culture] and Risk specialists to support consistency of decision making at a leadership level.

Policy specific

3.36 APRA policies reviewed in this audit typically include details of the consequences for non-compliance.

3.37 The APRA Code of Conduct states that:

If you breach the standards of conduct set out in the Code, you may face disciplinary action up to, and including, termination of employment.

3.38 The Conflicts of Interest Framework policy states that non-compliance not only breaches that policy but also constitutes a breach of the Code of Conduct. The Conflicts of Interest Framework policy states that:

Where a breach occurs, it will also be referred to the Employment Relations & Wellbeing team in P&C [People and Culture] and subject to consideration for consequence management actions and potential disciplinary action. Such a breach will be raised as an anonymised incident in APRA's risk management system and reported to the Executive Committee as part of the incident reporting framework.

3.39 The Financial Holdings Disclosure Policy (FHD) outlines the penalties for breaches of the policy.¹⁶⁶ At a minimum, APRA employees in breach of the FHD policy are:

to be cautioned by their relevant ED [Executive Director], with a formal record retained in their personnel file. Depending on the nature of the breach, further disciplinary action may be taken. All breaches must be reported to the Chief Risk Officer as reportable incidents.

3.40 Where equity holdings have been acquired in breach of the FHD policy, 'the APRA employee may be instructed by the relevant ED [Executive Director] to immediately divest the investment, provide evidence of the divestment and take any additional remediation actions their ED [Executive Director] considers necessary.'¹⁶⁷

3.41 APRA's policies for procurement, credit cards, and gifts, benefits and hospitality are contained in the APRA Chair's Finance Instructions and Policies (CFIs). These state that:

166 The FHD policy states that APRA's policy in relation to financial interests is as follows: 'APRA employees must not improperly use or disclose information obtained in the course of their work at APRA. This obligation is imposed on all employees under APRA's Code of Conduct, the relevant provisions of the APRA Act (secrecy provisions), the Corporations Act (including insider trading or tipping prohibitions), the Criminal Code Act (secrecy of information) and the common law.'

167 For example, APRA may impose conditions on the basis on which the divestment is to occur and/or how any profits from divestment are to be dealt with. Any loss that arises from the imposition of such conditions is to be borne by the employee.

Officials who breach the requirements of the PGPA Act [Public Governance, Performance and Accountability Act 2013], the CFIs or other statutory requirements will be investigated and the matter referred to the Chair for appropriate action. Action may include:

- (a) referral to Police or other authorities for prosecution;
- (b) termination of employment; and/or
- (c) other disciplinary action.

3.42 The CFIs also state that:

- all instances of non-business use of a corporate credit card are a breach of the PGPA Act and are required to be reimbursed within the statement period and reported to APRA Members; and
- the 'CFO [Chief Financial Officer] may suspend a card at any time for misuse or non-acquittal. Any amounts due to the Commonwealth will be settled immediately.'

3.43 APRA advised the ANAO that individuals who repeatedly offend against credit card requirements are escalated to their General Manager or Executive Director (although this is not referenced in APRA's credit card policy or guidance).¹⁶⁸ APRA further advised that there were two instances of 'multiple credit card misuse' during 2022–23. APRA documentation indicates that one instance was raised to a General Manager and one instance was raised to an Executive Director.

3.44 In respect to the consequences of fraudulent activity, APRA's CFIs state that:

Fraud against the Commonwealth and APRA is a very serious offence and can result in penalties under the *Crimes Act 1914* and the *Proceeds of Crime Act 1987*. Staff who commit fraud may also face misconduct charges under the APRA Terms and Conditions of employment and face loss of superannuation entitlements under the *Crimes (Superannuation Benefits) Act 1989*.

3.45 Identification of probity related non-compliance and the management of identified non-compliance is discussed in Chapter 4 of this audit report.

¹⁶⁸ APRA advised the ANAO in January 2023 that misuse of a credit card, including use for transactions that are private in nature, above limits specified in guidance and for repeat offenders, trigger this escalation.

4. Compliance with requirements

Areas examined

This chapter examines whether the Australian Prudential Regulation Authority (APRA) has demonstrated compliance with its probity requirements and addressed non-compliance in accordance with its stated requirements.

Conclusion

While APRA fully or largely complied with most of the probity related requirements examined in this audit, there was partial compliance with requirements for the use of corporate credit cards.

There is evidence that APRA has addressed identified non-compliance with the APRA Code of Conduct, conflict of interest requirements, the disclosure of financial holdings policy, and some instances of non-compliance relating to corporate credit card use.

Areas for improvement

The ANAO made one recommendation in relation to gifts, benefits and hospitality aimed at strengthening the transparency of internal reporting and ensuring that APRA's policy better meets the intent of its internal principle that officials should generally seek to avoid the receipt of gifts and offers of hospitality.

The ANAO also identified two opportunities for improvement aimed at: better meeting the intent of policy arrangements regarding the acceptance of gifts or offers of hospitality of a repetitive nature; and enhancing disclosure in APRA's internal register of gifts, benefits and hospitality in relation to gifts retained by individuals, surrendered to APRA or disposed of in some other way.

4.1 Entities cannot effectively manage probity related risks if the policies, procedures and arrangements designed to mitigate those risks are not followed. This chapter assesses whether APRA has demonstrated compliance with the probity requirements selected for ANAO review and addressed non-compliance in accordance with its stated requirements.

4.2 The requirements reviewed by the ANAO related to:

- the APRA Code of Conduct;
- conflict of interest and disclosure of financial holdings;
- senior executive remuneration;
- selected procurement requirements;
- corporate credit card use; and
- gifts, benefits and hospitality.¹⁶⁹

Has APRA complied with the selected probity requirements?

For the periods reviewed by the ANAO, APRA undertook its internal assurance processes under which relevant personnel made declarations relating to the APRA Code of Conduct and compliance with conflict of interest and financial trading requirements. Results for the respective processes were reported to senior management committees. Disclosures of APRA

¹⁶⁹ The ANAO did not test APRA's compliance with public interest disclosures.

Members' interests were provided to the Treasurer as required under the *Australian Prudential Regulation Authority Act 1998*.

APRA personnel largely complied with requirements relating to gifts, benefits and hospitality. For a sample of credit card transactions reviewed, there was partial compliance with requirements relating to corporate credit card use.

APRA did not have a specific policy for managing senior executive remuneration, but advised that the general policy applying to staff was applied to its senior executives in practice. At a high level, the process APRA adopted for senior executive remuneration was consistent with the general staff remuneration policy. There is evidence that the APRA Chair was provided with information on, and approved, individual remuneration outcomes for all members of the senior executive cohort for the most recent review process that involved a pay rise.

APRA's procurement policies and guidance require officials to comply with the Commonwealth Procurement Rules (CPRs). APRA's procurement policies and guidance do not outline any further specific requirements for the management of probity related risks. For the ten high-value procurements reviewed by the ANAO, APRA documented the requirement to consider probity as part of the procurement process in seven cases. Two of the 10 procurements examined were incorrectly reported on AusTender and for one procurement, the evaluation criteria limited competition contrary to the requirements of the CPRs.

There is scope for APRA to enhance its requirements in relation to gifts, benefits and hospitality.

Compliance with annual declaration requirement relating to the APRA Code of Conduct

4.3 APRA's Code of Conduct arrangements are discussed in paragraphs 2.3 to 2.9. Individuals subject to APRA's Code of Conduct are required to acknowledge they have read and understood the Code of Conduct at least annually.

4.4 The ANAO examined whether there was evidence of individuals subject to APRA's Code of Conduct having completed the annual declaration for the most recent annual process.

4.5 APRA records indicate that APRA conducted its annual declaration process in 2022 and the completion rate for making the annual code of conduct declaration was monitored. The due date for the declaration was 30 June 2022.

4.6 APRA records indicate that: as at 1 July 2022, 48 people required to complete the annual declaration had not done so¹⁷⁰; and by 26 August 2022 all people required to complete the declaration had done so.¹⁷¹ There is evidence that APRA followed up with individuals who had not completed the declaration.

4.7 APRA advised the ANAO in January 2023 that APRA management is provided with completion rates for the Annual Conflicts of Interest declaration campaign via reporting to its Executive Committee. APRA further advised that management is not provided with completion

170 This equated to approximately six per cent of staff.

171 APRA records indicate that this was 'net of people on long-term leave and on inter-agency secondment.'

rates for new staff conflict of interest declaration completions, as these are monitored for completion on a real-time basis by APRA's Risk Management and Compliance team.¹⁷²

Compliance with annual declaration process requirements relating to conflict of interest and financial holdings disclosure

4.8 APRA's arrangements for managing conflict of interest and disclosing financial holdings are discussed in paragraphs 2.10 to 2.25 and 2.37 to 2.45 respectively.

4.9 As discussed in paragraph 2.22, individuals subject to APRA's Conflicts of Interest Framework have an ongoing requirement to disclose conflicts of interests as they arise. In addition to this ongoing requirement, APRA Members and employees are required to complete an annual declaration on conflict of interest. The annual declaration requirements were discussed in paragraph 2.20 and include the need to disclose information relating to direct security holdings in APRA-regulated entities and changes to holdings.

4.10 The ANAO examined whether there is evidence of APRA having conducted its annual declaration process relating to conflict of interest and disclosure of financial holdings for the most recent period, and whether the results were reported to relevant senior management. The ANAO also examined what actions APRA took in relation to identified non-compliance (this is discussed further in paragraphs 4.57 to 4.58).

4.11 At the time the ANAO conducted audit fieldwork, the most recent completed annual declaration cycle was 30 November 2022. APRA documents indicate that it had identified four breaches arising from the November 2022 process. These breaches were reported to the Executive Committee in March 2023.

Disclosure of Members' interests

4.12 Under section 48A of the *Australian Prudential Regulation Authority Act 1998*, APRA Members have a standing obligation to disclose certain interests to the Minister in writing. APRA's practice is to provide a letter to the Treasurer on an annual basis providing Members' disclosures. The APRA Chair provided an annual disclosure of interests letter to the Treasurer on 3 August 2021 and 19 July 2022. The Chair provided an updated letter on 29 November 2022 after the appointment of two new APRA Members.

Compliance with senior executive remuneration requirements

4.13 APRA's arrangements for senior executive remuneration are discussed in paragraphs 2.50 to 2.61. As noted in paragraph 2.51, APRA did not have a policy for managing senior executive remuneration. As a result, the ANAO was unable to test whether APRA's process for reviewing senior executive remuneration for its most recent performance period was undertaken in accordance with specific entity requirements.

172 APRA advised the ANAO that if there is an issue with completion, the Risk Management and Compliance team follows up directly with the staff member, and if overdue status continues, escalation will occur to the Line manager/General Manager and Executive Director as necessary. When a new staff member completes their first conflict of interest declaration, the financial holdings declaration and any non-financial disclosure made is sent to the relevant Executive Director.

4.14 As discussed in paragraph 2.52, APRA advised the ANAO that while its Remuneration Review Policy (dated June 2022) is intended for staff and does not cover senior executives, in practice the principles outlined in the policy are applied to the senior executive cohort.

4.15 The ANAO reviewed whether:

- at a high level, the process for reviewing senior executive remuneration generally reflected the process applied to staff, as outlined in APRA's June 2022 Remuneration Review Policy, notwithstanding that the policy does not apply to the senior executive cohort¹⁷³; and
- APRA's accountable authority (the APRA Chair) was provided with and approved individual remuneration outcomes for members of the senior executive for the most recent performance cycle that resulted in a pay rise.

4.16 For the purposes of audit testing, APRA's senior executive refers to General Managers and Executive Directors.¹⁷⁴ In summary, there is evidence that APRA's process for reviewing senior executive remuneration for its most recent cycle generally reflected the process applied to APRA staff. There is also evidence that the APRA Chair was provided with information on, and approved, individual remuneration outcomes for all members of the senior executive cohort for the most recent performance cycle or review process that involved a pay rise.

4.17 APRA utilises a remuneration model to support its annual review of remuneration for all staff. As part of this process, staff roles in APRA are assessed for capability¹⁷⁵ and roles are also mapped to internal and external benchmarks. The remuneration model used for APRA's 2022 review process is used to support recommended remuneration outcomes for each individual that, amongst other things, takes into account: a guaranteed 5.5 per cent increase¹⁷⁶; their performance; their remuneration relative to the internal and external benchmarks; and whether the role was considered a promotion.¹⁷⁷

4.18 For the General Manager cohort, APRA advised the ANAO that APRA Executive Directors separately submitted General Manager recommendations for the 2022 remuneration process, reviewing current remuneration position and internal and external benchmark data. Following this, joint meetings between Executive Directors and APRA's People and Culture representatives were

173 As discussed in paragraph 2.52, the policy does not state that it applies to senior executives, and not all the steps in the policy are applicable to the senior executive cohort.

174 In APRA's organisation structure, Executive Directors supervise General Managers.

175 APRA advised the ANAO that the APRA Capability Framework does not include the General Manager and Executive Director levels. In the model, General Managers are assigned a capability stream as either tier one or tier two. The difference relates to the role undertaken. Individuals undertaking a larger role are given a ranking of two and those undertaking a smaller role are given a ranking of one. Within those tiers General Managers are given a capability assessment of either low, medium or high. APRA advised the ANAO that these rankings are decided following discussions with APRA Members and APRA Executive Directors. APRA advised that there are also three General Manager roles that sit outside the two tiers of General Manager pay ranges, where 'the skillset and market drive the remuneration paid'. In the model, Executive Directors are all assigned the same capability stream of 'Executive' and there is no capability assessment (for example low, medium or high) recorded in the model.

176 APRA advised the ANAO that the guaranteed 5.5 per cent increase related to the roll-in of performance bonuses, discussed in paragraphs 2.57 to 2.59, was applied to all eligible employees (and senior executives).

177 The remuneration model includes employee data such as name, role, gender, tenure, capability (for General Managers), existing remuneration, internal and external benchmarks, proposed increases, and any reasons where there were adjustments made.

held.¹⁷⁸ APRA advised the ANAO that: ‘An initial meeting with the APRA Chair was held to confirm progress in the remuneration review and confirm that he was comfortable with recommendations. This included sharing the remuneration tool and summary data sets.’ APRA records indicate that the APRA Chair was emailed details of the proposed remuneration outcomes for the General Manager cohort and approved them. The APRA Chair was also advised that the overall percentage increase for General Managers was nine per cent.¹⁷⁹

4.19 For the Executive Director cohort, APRA advised the ANAO that the General Manager People and Culture met with the APRA Chair and Members to discuss Executive Director performance and their proposed increases. APRA documentation indicates that subsequent to the discussion the General Manager People and Culture emailed the APRA Chair seeking approval of the proposed remuneration outcomes (on average 9.3 per cent) for the Executive Director cohort¹⁸⁰, which the Chair approved.

4.20 As of March 2023, no further increases in remuneration to members of the senior executive had occurred.

Consideration of probity in procurement

4.21 APRA’s policies, guidance and arrangements for probity management in procurement activities are outlined in paragraphs 2.62 to 2.72.

4.22 APRA’s procurement policies and guidance require officials to comply with the CPRs.¹⁸¹ As discussed in paragraph 2.66, for the period reviewed in this audit APRA’s procurement policies and guidance did not include any further specific requirements for the management of probity related risks. In November 2022 APRA advised the ANAO that it has introduced a requirement to confirm that its central procurement team will be notified should anyone involved in a selection process have any conflicts of interest with any of the suppliers being evaluated (see paragraph 2.68).

4.23 The ANAO selected a sample of ten procurements undertaken by APRA between July 2021 and October 2022. The procurements selected were the 10 highest value procurements for the period recorded on AusTender as at 19 October 2022.

4.24 For each procurement, the ANAO assessed whether there was evidence of the consideration of probity as part of the procurement process. The results of this assessment are summarised in Table 4.1.

178 APRA advised the ANAO that the intent of these meetings was to take a joint approach to the final remuneration recommendations for General Managers, to ensure consistency and alignment across the cohort as well as consideration of the overall budget position of the proposed increases. People and Culture is the area within APRA that has responsibility for employment-related matters.

179 This includes the guaranteed five and a half per cent increase related to the roll-in of performance bonuses.

180 The email from the General Manager People and Culture advised the Chair that the information was modelled on providing the same standard increase of 5.5 per cent that was applied to staff relating to the roll-in of performance bonuses (as discussed in paragraph 4.17) and an average additional increase of 3.8 per cent to the Executive Directors.

181 While the CPRs contain clear statements regarding the need for ethical behaviour, they do not set out specific operational requirements. Where an accountable authority considers that there is a need for specific operational requirements, this is generally done in the context of accountable authority instructions.

Table 4.1: Consideration of probity in the selected APRA procurements

Sample number	Procurement and Contract Notice (CN) number	Procurement type as assessed by the ANAO	Value at 19/10/22 as recorded on AusTender (\$)	ANAO comment
1	IT Maintenance – Software maintenance and support (CN3814388-A4)	Open tender	5,366,578	<ul style="list-style-type: none"> Procurement method recorded on AusTender was open tender. An approach to market was undertaken in July 2018. APRA provided probity declarations relating to the 2018 approach to market.
2	IT Services – Internet services (CN3800857)	Panel procurement – single supplier approached	4,499,636	<ul style="list-style-type: none"> APRA documentation indicates that this procurement was an extension of an existing contract (CN3751621), however it was reported as a separate contract. Procurement Team representative identified.^a There was no documented evidence of probity management specific to this procurement.
3	Legal services (CN3814397)	Open tender	1,500,000	<ul style="list-style-type: none"> There was documented evidence of engagement with APRA procurement specialists. Evaluation team members were advised of the need to declare conflicts of interest with potential suppliers. In response, one declaration was made identifying potential conflicts of interest and the relevant person did not continue on the evaluation team.
4	IT Maintenance – Electronic hardware and component parts and accessories (CN3903882)	Panel procurement – three suppliers approached	1,429,818	<ul style="list-style-type: none"> Procurement Team representative identified. The official submitting the procurement request ticked a box on the workflow that the 'Requestor promise to declare COI [conflict of interest]'.
5	IT Maintenance – Software maintenance and support (CN3860263)	Limited tender – single supplier approached	1,208,932	<ul style="list-style-type: none"> The procurement method recorded on AusTender as 'open tender' while APRA documentation indicates that this was a limited tender procurement. APRA advised the ANAO that this procurement should have been reported as a limited tender.

Sample number	Procurement and Contract Notice (CN) number	Procurement type as assessed by the ANAO	Value at 19/10/22 as recorded on AusTender (\$)	ANAO comment
				<ul style="list-style-type: none"> Procurement Team representative identified. There was no documented evidence of probity management specific to this procurement.
6	Personnel Services – Temporary personnel services (CN3814394-A1)	Panel procurement – four suppliers approached	1,075,685	<ul style="list-style-type: none"> Documented evidence of engagement with APRA procurement specialists. Staff involved in the evaluation process were advised of the requirement to report any potential conflicts of interest with potential suppliers. The evaluation report stated that ‘The members of the ET [Evaluation Team] have declared that they do not have pecuniary or non-pecuniary interests in the organisations responding to the RFQ [Request for Quote]’. Records of declarations were not kept.
7	IT Security and Network Engineer Contractors – Temporary personnel services (CN3885202)	Panel procurement – three suppliers approached	900,359	<ul style="list-style-type: none"> Procurement Team representative identified. Staff involved in the evaluation process were advised of the requirement to report any potential conflicts of interest with potential suppliers. The evaluation report stated that ‘The members of the ET have declared that they do not have pecuniary or non-pecuniary interests in the organisations responding to the RFQ [Request for Quote]’. Records of declarations were not kept.
8	Contractor – Temporary personnel services (CN3800845-A1)	Panel procurement – four suppliers approached	638,379	<ul style="list-style-type: none"> Procurement Team representative identified. Staff involved in the evaluation process were advised of the requirement to report any potential conflicts of interest with potential suppliers.
9	Personnel Services	Panel procurement –	637,670	<ul style="list-style-type: none"> Procurement Team representative identified.

Sample number	Procurement and Contract Notice (CN) number	Procurement type as assessed by the ANAO	Value at 19/10/22 as recorded on AusTender (\$)	ANAO comment
	(CN3814384-A2)	four suppliers approached		<ul style="list-style-type: none"> Staff involved in the evaluation process were advised of the requirement to report any potential conflicts of interest with potential suppliers.
10	Building Works – Refurbishing services (CN3915858)	Panel procurement – four suppliers approached	599,441	<ul style="list-style-type: none"> Procurement Team representative identified. APRA documentation indicates that four suppliers were approached, but only one of these was on the panel that APRA used. APRA's criteria for assessing the suppliers included the tenderers' 'experience working with APRA' and whether the tenderers were 'on government panel and/or indigenous supplier'. These criteria do not meet the requirements of paragraph 5.4 of the CPRs.^b There was no documented evidence of probity management specific to this procurement.

Note a: In this table, 'Procurement Team representative identified' indicates there is evidence that someone from APRA's central procurement team was involved in the procurement.

Note b: CPR paragraph 5.4 states that 'All potential suppliers to government must, subject to these CPRs, be treated equitably based on their commercial, legal, technical and financial abilities and not be discriminated against due to their size, degree of foreign affiliation or ownership, location, or the origin of their goods and services.'

Source: ANAO review of APRA documentation.

4.25 As summarised in Table 4.1, for the ten high-value procurements reviewed by the ANAO, APRA documented the requirement to consider probity as part of the procurement process in seven cases.¹⁸² As discussed in paragraph 2.71, there is an opportunity for APRA to improve its guidance regarding the consideration of probity in procurement. A revised approach would provide assurance that probity has been considered in every procurement.

4.26 The ANAO's review also identified that:

182 For:

- sample one, probity declarations were completed by evaluation team members;
- sample four, the official submitting the procurement request ticked a box on the workflow that the 'Requestor promise to declare COI [conflict of interest]; and
- for five procurements (samples three, six, seven, eight and nine) evaluation team members were advised of the need to declare conflicts of interest. In sample three, one declaration was made identifying potential conflicts and in samples six and seven, the evaluation report stated there were no conflicts, although records of declarations were not kept.

There was no documented evidence of probity management in relation to samples two, five and ten.

- one of the selected procurements was reported on AusTender as open tender when it was a limited tender procurement¹⁸³;
- one procurement for an existing contract was reported on AusTender as a new contract¹⁸⁴; and
- one contract included evaluation criteria that limited competition from the outset, which is inconsistent with the intent of the CPRs.¹⁸⁵

Compliance with corporate credit card requirements

4.27 APRA's policies, procedures and arrangements for credit card expenditure were discussed in paragraphs 2.73 to 2.96.

4.28 The ANAO examined the corporate credit use of the following senior APRA personnel:

- the Accountable Authority;
- the Deputy Chairs; and
- Chief Operating Officer (COO).

4.29 These roles were selected on the basis that setting the 'tone at the top' is important when trying to instil an ethical culture in an entity. Further, external review is a means of testing whether there are controls in place to manage positional authority risks within an entity.¹⁸⁶

4.30 The ANAO also examined whether the executive assistants for people in the above roles have credit cards and if so, whether they can make purchases on behalf of their manager.

4.31 The ANAO reviewed all credit card transactions for the people in the selected roles for the months of June and July 2022. These months were selected as they were sufficiently recent to reflect current entity practices and, at the time of conducting audit testing, the acquittal process should have been complete. The ANAO examined whether:

- transactions were acquitted within the required timeframe;
- tax invoices or other supporting documentation was provided (where applicable);
- transactions were approved in accordance with requirements; and
- whether transactions appeared to be for incidental or other private expenditure.

4.32 In the audit sample there were 106 credit card transactions, with a total expenditure of \$56,141.98. Of the 106 transactions examined, 42 (39.6 per cent) were found to be non-compliant with APRA's requirements.¹⁸⁷ The specific non-compliances were as follows.

- In 30 instances transactions were not acquitted by the 20th day of the following month, as required by APRA's guidance.

183 Sample number five.

184 Sample number two.

185 Sample number 10.

186 The COO was selected as a key senior executive in relation to managing the entity and is typically responsible for many of the probity related risks examined in this audit.

Positional authority risks are discussed further in paragraphs 2.82 to 2.86 of this audit report.

187 Five instances of identified non-compliance are listed in more than one category as they were non-compliant with multiple credit card requirements.

- In three instances a transaction was for a journal or publication subscription.¹⁸⁸
- In four instances there were no tax receipts provided as required. Of these, there were two instances where APRA records indicate tax receipts had been provided but no evidence of receipts was provided to the ANAO.
- In three instances an APRA Member's transaction was approved by a subordinate (one by a General Manager and two by a cost centre manager¹⁸⁹) instead of a Member.
- In seven instances, Member transactions were approved by another Member but not in accordance with the established approval requirements.¹⁹⁰

4.33 The ANAO identified 13 transactions where a manager approved expenses incurred on their executive assistant's card. APRA advised the ANAO that managers can approve the expenses of their executive assistants but are not to approve their own expenses. APRA further advised the ANAO that it was unable to identify instances where an executive assistant had made a purchase on behalf of their manager.

4.34 For the 106 transactions reviewed by the ANAO, no instances were observed that appeared to be for private expenditure.

Compliance with gifts, benefits and hospitality requirements

4.35 APRA's arrangements for gifts, benefits and hospitality are discussed in paragraphs 2.97 to 2.103.

4.36 The ANAO reviewed APRA's gifts, benefits and hospitality register for the period 1 July 2020 to 30 September 2022. The ANAO examined the register for this period because the effective management of probity risks related to gifts, benefits and hospitality is an important element of: supporting an ethical culture; managing the risk of real and perceived conflicts of interest; and managing the risk of regulatory capture.

4.37 The ANAO examined whether:

- declarations were made in line with APRA policy;
- gifts, benefits or hospitality to staff were approved in accordance with requirements; and
- where applicable, details of gifts, benefits and hospitality reported on APRA's website matched those on APRA's internal register.

4.38 There were 98 entries in APRA's register, of which: 93 were recorded as accepted; two were recorded as gifted by APRA; one was recorded as declined; and two were recorded as 'expired'

188 APRA advised the ANAO in January 2023 that 'Non-reimbursable items are not allowed to be purchased under APRA's credit card policy.' APRA's Talent and Employment Policy states that: 'Subscriptions to professional journals and publications are not reimbursable.'

189 APRA advised the ANAO that: 'There was an oversight on 2 of the transactions which were approved by the cost centre manager incurring the expense. These 2 transactions were for minor business as usual expenses.' APRA requires the Finance team to be advised when there are exceptions made to the 'circular approval' arrangements. No evidence was provided to the ANAO demonstrating that the Finance team was advised of these exceptions.

190 APRA's 'circular approval' process is discussed in paragraph 2.85. APRA advised the ANAO that: 'For transactions where the circular arrangements have not been followed, it was due to the relevant approver being either on annual leave or overseas at the time.'

(entered in error). Thirty three per cent of declarations related to the acceptance of a gift. This was the largest category in the register.

4.39 Table 4.2 provides a summary of entries in APRA's gifts, benefits and hospitality register during the period reviewed by the ANAO.

Table 4.2: Summary of APRA's gifts, benefits and hospitality register

Category ^a	Number	Percentage	Examples
Complimentary attendance at a conference, presentation or seminar	16	16	<ul style="list-style-type: none"> Discounted or free registration to attend a presentation or conference. Presenters at a conference or seminar received a free ticket to attend the rest of the event.
Functions and events	15	15	<ul style="list-style-type: none"> Attendance at cocktail parties/drinks events. Attendance at speaking events as the guest of industry peak bodies. Provided with tickets to functions. Attendance at evening networking/drinks events. Attendance at awards dinners.
Meals	26	27	<ul style="list-style-type: none"> Dinners hosted by conference organisers pre or post conference. Breakfast meeting. Invitation to an annual awards dinner. Working lunch while in attendance at a meeting. Lunches provided by suppliers. Attendance at boardroom luncheon events hosted by stakeholders.
Gifts	32	33	<ul style="list-style-type: none"> Bottles of wine. Bottles of champagne. Desktop wireless chargers. USB microphones. Food hampers. Gift boxes. Self-care packages. Umbrellas. Gift vouchers. Donations to charity on behalf of an APRA official.
Cultural Gifts ^b	4	4	<ul style="list-style-type: none"> Commemorative bookmarks. Calendar from an embassy.
Total accepted and approved items	93		

Category ^a	Number	Percentage	Examples
Gifted by APRA	2	2	<ul style="list-style-type: none"> Entry by a former colleague to an airline lounge (membership paid for by APRA). Two \$50 gift cards gifted to a charity.
Declined	1	1	
Expired	2	2	<ul style="list-style-type: none"> Entry created in error. Confirmed with the staff member it was entered as a mistake, then the entry was closed.
Total entries^c	98	100	

Note a: The categories in this table were determined by the ANAO based on analysis of APRA's Gifts, Benefits and Hospitality register.

Note b: Cultural gifts are items of cultural or sentimental value for which a monetary value is difficult to assign.

Note c: APRA advised the ANAO in January 2023 that no airline lounge memberships were declared during the audit review period. In February 2023, APRA updated its website information relating to Members, for the period 1 October 2022 to 31 December 2022. This included an entry declaring complimentary lounge memberships or lounge access for Members.

Source: ANAO analysis of APRA's gifts, benefits and hospitality register, 1 July 2020 to 30 September 2022.

4.40 In respect to the entries in APRA's register for the period reviewed, most gifts, benefits and hospitality were managed in accordance with APRA requirements.¹⁹¹ The ANAO identified the following exceptions.

- There were two occasions, involving entries with a reported value of \$100, where the entry in the register stated that approval was not needed.¹⁹² At the time these gifts were declared, APRA's policy required items of \$100 or more to be approved.¹⁹³
- There were two occasions where an entry with a value of \$100 was not reported on the APRA website in accordance with APRA requirements.¹⁹⁴ There was one occasion where an entry of \$200 was not reported on the APRA website.

191 APRA's requirements are summarised in Chapter 2 in Table 2.2.

192 APRA advised the ANAO in January 2023 that for these two instances 'The system workflow was not aligned to the CFI [Chair's Finance Instructions and Policies] policy requirement. It has now been aligned'.

193 The March 2020 CFIs (the version applicable at the time the gift was received) stated that: 'where the gift value is \$100 or more, an approval will be required from your ED [Executive Director]. Approval is required from an APRA Member for gifts or hospitality valued at \$100 or more that are received by EDs [Executive Directors].' As discussed in paragraph 2.85, APRA Members follow APRA's circular approval arrangements.

194 At the time of audit field work, the APRA website stated that gifts of \$100 and over were reported on the website. This description on the website was amended in February 2023 to state that APRA is reporting gifts over \$100.

- There were three occasions where different employees accepted two offers of gifts, benefits or hospitality from the same source with a combined value of \$100 or higher within a six-month period.¹⁹⁵ These instances involved employees doing the following.
 - Receiving two gifts from a cleaning service provider, which were declared in the register on the same day. One was valued at \$70 and the second was valued at \$80.
 - Attending two events at the invitation of an education provider within a six-month period. The first was valued at \$75 and was accepted in December 2021. The second was valued at \$105 and was accepted in March 2022.
 - Receiving a bottle of wine and lunch from the landlord for one of APRA's office sites. The wine was valued at \$60 and was received in December 2021. The lunch was valued at \$120 and was accepted in May 2022.¹⁹⁶ These were declarations made by the COO.¹⁹⁷

4.41 The APRA Chair's Finance Instructions and Policies (CFIs) state that where gifts or offers of hospitality are given to officials 'in a repetitive nature', the official should seek to ensure this remains inside the \$100 threshold in total, or otherwise decline (see footnote 195). The repeated acceptance of gifts or offers of hospitality from the same source (including by APRA's most senior officials, as discussed in paragraph 4.40, last dot point), indicates that there is scope for APRA to consider further how best to ensure that officials meet the intent of the CFIs.

Opportunity for improvement

4.42 There is an opportunity for the Australian Prudential Regulation Authority to consider ways to better meet the intent of the CFI provision regarding the acceptance of gifts or offers of hospitality of a repetitive nature.

4.43 As noted in paragraph 2.100, the CFIs state that:

Officials should, as a general rule, seek to avoid the receipt of gifts and offers of hospitality or sponsored travel where possible.

Officials must not accept gifts, offers of hospitality or sponsored travel, regardless of value, if the APRA official may have an actual or perceived conflict of interest as a result of receiving the gift.

195 The March 2020 CFIs (the version applicable at the time of each occasion) stated that: 'Where gifts or offers of hospitality are given to officials in a repetitive nature (assessed on a rolling 6 month basis), the official should seek to ensure this remains inside the \$100 threshold in total, or otherwise decline.'

The August 2022 version of the CFIs (the version in place at the time of audit fieldwork) states the following.

- For gifts: 'Where minor gifts are given to officials in a repetitive nature (assessed on a rolling 6 month basis), the official should seek to ensure this remains inside the \$100 threshold in total, or otherwise seek to refuse acceptance.'
- For hospitality: 'Where small instances of hospitality are given to officials in a repetitive nature (assessed on a rolling 6 month basis), the official should seek to ensure this remains inside the \$100 threshold in total, or otherwise seek to refuse acceptance.'

196 The gift was reported as received during the Christmas–New Year period of 2021 and APRA records indicate that the gift was declared in the register on 1 March 2022. The lunch is reported as accepted on 24 May 2022. These entries are also discussed in paragraph 4.46.

197 See paragraph 4.60 for detail of APRA advice regarding how to address identified non-compliance.

4.44 For officials of a regulatory entity, there is a risk that accepting any gift, benefit or hospitality from a regulated entity could be perceived as a conflict of interest. As discussed in paragraph 2.98, perceptions of this sort can give rise to reputational risks, including the legitimacy and integrity of the regulator.

4.45 A number of the items on APRA's gifts, benefits and hospitality register were recorded as being offered by entities regulated by APRA. These included:

- attendance at a cocktail event for the outgoing Chair of the Commonwealth Bank of Australia;
- dinner and transport costs for travel to the dinner venue provided by Munich Re Australia;
- complimentary tickets provided by the Westpac Banking Corporation¹⁹⁸;
- five umbrellas provided by the Westpac Banking Corporation;
- a bottle of wine provided by Mercer Australia; and
- a dinner event provided by Mercer Australia.

4.46 A number of the items on APRA's gifts, benefits and hospitality register were recorded as being offered by APRA suppliers. These included:

- lunches provided by the landlord of one of APRA's office sites¹⁹⁹;
- bottles of wine provided by the landlord at one of APRA's office sites;
- food hampers provided by an actuarial firm to two APRA officials; and
- a gift box provided by a recruitment firm.

4.47 APRA's declaration process does not require recipients to document in the gifts, benefits and hospitality register their assessment of whether accepting an offer represents a real or perceived conflict of interest. In effect, there is no record of the basis for the individual official's decision. APRA can strengthen its arrangements for managing reputational risk by requiring the recipients of offers of gifts, benefits and hospitality to record in the internal register whether accepting the offer represents a real or perceived conflict of interest and document the basis for their decision. Documenting the basis of decisions is particularly important for managing perceptions of conflicts of interest related to the acceptance of such offers from regulated entities and the suppliers of goods and services.

4.48 APRA should also review whether its policy settings align with the internal principle, established in the CFIs, of officials generally seeking to avoid the receipt of gifts and offers of hospitality.

198 This was described in APRA's gifts, benefits and hospitality register as 'complimentary ticket to the National Press Club Gallery in Canberra', with a declared value of \$99. The threshold for requiring approval and publishing details for the gift on APRA's website is \$100.

199 This included lunches on 4 March 2021 and 24 May 2022. APRA's website indicates that prior to the period examined in this audit (1 July 2020 to 30 September 2022) there were also lunches provided by the same supplier on 16 July 2019 and 11 December 2019. Additionally, lunches from the same supplier took place in December 2022.

Recommendation no. 2

4.49 The Australian Prudential Regulation Authority strengthen its gifts, benefits and hospitality arrangements by:

- (a) requiring the recipients of offers of gifts, benefits and hospitality to record in the internal register whether accepting the offer represents a real or perceived conflict of interest and document the basis for their decision to accept; and
- (b) reviewing whether its policy settings adequately support the established internal principle of officials generally seeking to avoid the receipt of gifts and offers of hospitality.

Australian Prudential Regulation Authority response: *Agreed.*

4.50 *APRA will consider avenues to further emphasise its policy expectations, and highlight additional instances where acceptance is not allowed. To strengthen the Policy stance of not accepting gifts regardless of whether the conflict is perceived or actual, APRA will include a requirement to specifically record that assessment.*

4.51 In the case of gifts, APRA's register does not include information on whether the individual making the declaration retained the gift, surrendered it to APRA, or disposed of it in some other way. While APRA maintains an inventory of gifts surrendered to APRA, it could improve the transparency of its internal register of gifts, benefits and hospitality by introducing requirements to capture this information.

Opportunity for improvement

4.52 The Australian Prudential Regulation Authority could record in its internal register whether gifts were retained by individuals accepting them, surrendered to APRA or disposed of in some other way.

Has non-compliance been addressed in accordance with stated requirements?

There is evidence that identified instances of non-compliance were addressed by APRA in accordance with its requirements for: breaches of the financial holdings disclosure policy; annual code of conduct declaration process; and annual declaration of conflicts of interest process.

There is evidence of some instances of non-compliance identified by APRA, or in the context of this audit, being addressed in accordance with APRA's requirements in relation to corporate credit card use.

There is no evidence of instances of non-compliance identified by APRA, or in the context of this audit, being addressed in accordance with APRA's requirements for: procurement; and gifts, benefits and hospitality.

4.53 Following up on identified instances of non-compliance assists in providing assurance to the accountable authority on compliance with entity requirements and the effectiveness of probity management arrangements.

4.54 APRA's framework for following up on identified instances of non-compliance is discussed in paragraphs 3.29 to 3.45.

4.55 The ANAO examined whether there was evidence of action being taken in relation to non-compliance identified by APRA and in the context of this audit.

Attestation process relating to APRA Code of Conduct

4.56 APRA conducted the annual code of conduct attestation process in accordance with its requirements. As outlined in paragraph 4.6, APRA records indicate that all people required to complete the declaration had done so for the most recent attestation period.²⁰⁰

Declaration process relating to conflict of interest and disclosure of financial holdings

4.57 APRA conducted the annual declaration process relating to conflict of interest and disclosure of financial holdings in accordance with its requirements. APRA demonstrated that completion rates were tracked and that individuals who had not completed the declaration were followed up until all those required to complete the declaration had done so.

4.58 As discussed in paragraph 4.11, APRA identified four breaches of its financial holdings policy. The ANAO examined what action APRA took in relation to the identified non-compliance. APRA records indicate that:

- two instances involved a staff member being issued a formal warning; and
- two instances involved an email reminder being sent to the staff member.

Procurement, use of corporate credit cards and gifts, benefits and hospitality

4.59 With regard to the non-compliance relating to credit cards, discussed in paragraph 4.32, APRA advised the ANAO in January 2023 that the following action was being undertaken:

Communication and reiteration of APRA's CFI's [the APRA Chair's Finance Instructions and Policies], processes and review to the supporting EAs [executive assistants] assisting in the administration of credit cards, with a focus on timeliness and relevant approvals occurs. Finance, Internal Audit and the Executive Office continue to strengthen processes to reduce future occurrences.

4.60 With regard to the non-compliance relating to gifts, benefits and hospitality, discussed in paragraphs 4.40 and 4.41, APRA advised the ANAO in January 2023 that:

RMC [Risk Management and Compliance] proposes to highlight the policy requirement in scheduled all staff communications in Aug and Dec 2023 and will monitor such instances and refer any further instances to the relevant ED [Executive Director] and [APRA] will amend the description on the APRA Website to state that we are reporting gifts over \$100.



Grant Hehir
Auditor-General

Canberra ACT
1 June 2023

200 APRA records note that this was 'net of people on long-term leave and on inter-agency secondment.'

Appendices

Appendix 1 Australian Prudential Regulation Authority response

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY

1 Martin Place (Level 12), Sydney, NSW 2000
GPO Box 9836, Sydney, NSW 2001

T 02 9210 3000 | W www.apra.gov.au



APRA

JOHN LONSDALE

Chair

10 May 2023

Grant Hehir
Auditor-General
Australian National Audit Office
GPO Box 707
CANBERRA ACT

Dear Grant,

PROBITY MANAGEMENT IN FINANCIAL REGULATORS – AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY (APRA)

I refer to your correspondence dated 18 April 2023. Thank you for the opportunity to respond to the matters raised in the proposed Report.

It is critical that APRA upholds the highest probity standards, and that our Board Members and Management prioritise this in all business engagements. APRA views the Report findings as an opportunity to develop and refine Probity Management processes and guidance, building on existing probity improvement initiatives.

It is pleasing to see that APRA's probity governance, risk management and compliance systems are largely effective. APRA agrees with the two recommendations presented in the report and are committed to implementing actions to address these. APRA will consider the practicality of implementing the identified opportunities for improvement, in accordance with the respective risk exposures.

I thank the Australian National Audit Office for its Report and the important work they are undertaking, to provide assurance to Parliament and the Australian community surrounding the proper use of public resources.

Yours sincerely,

Appendix 2 Improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur: in anticipation of ANAO audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.

2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's 2022–23 Corporate Plan states that the ANAO's annual performance statements will provide a narrative that will consider, among other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.

3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:

- strengthening governance arrangements;
- introducing or revising policies, strategies, guidelines or administrative processes; and
- initiating reviews or investigations.

4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been appropriately implemented. Changes observed include the following.

- Updates to the following policies and frameworks:
 - Chair's Finance Instructions, with updates to areas relating to receiving gifts, donations, offers of hospitality and sponsored travel;
 - Compliance Management Policy;
 - Conflicts of Interest Framework;
 - Reportable Incident and Escalation Standards; and
 - Professional and Ethical Behaviour Policy.
- Introduction of Supervision Tenure Guidance as a key control to mitigate risk of regulatory capture and key divisional risks.

Appendix 3 Department of Finance guidance — Ethics and Probity in Procurement: Principles

1. An extract of the Department of Finance’s guidance on ‘Ethics and Probity in Procurement: Principles’²⁰¹ is reproduced below.

1. The principles underpinning ethics and probity in Australian Government Procurement are:

- Officials must act ethically, in accordance with the APS Values (set out in section 10 of the Public Service Act 1999) and Code of Conduct (set out in section 13 of the Public Service Act 1999), at all times in undertaking procurement.
- Officials must not make improper use of their position.
- Officials should avoid placing themselves in a position where there is the potential for claims of bias.
- Officials must not accept hospitality, gifts or benefits from any potential suppliers.
- Agencies must not seek to benefit from supplier practices that may be dishonest, unethical or unsafe, which may include tax avoidance, fraud, corruption, exploitation, unmanaged conflicts of interest and modern slavery practices.
- All tenderers must be treated equitably. This means that all tenderers must be treated fairly - it does not necessarily mean that they are treated equally.
- Conflicts of interest must be managed appropriately.
- Probity and conflict of interest requirements should be applied with appropriate and proportionate measures informed by sound risk management principles.
- Value for money outcomes are best served by effective probity measures that do not exclude suppliers from consideration for inconsequential reasons.
- Confidential information must be treated appropriately during and after a procurement process.
- External probity specialists should only be appointed where justified by the nature of the procurement.

201 Department of Finance, *Ethics and Probity in Procurement: Principles* [Internet], 17 May 2021, available from <https://www.finance.gov.au/government/procurement/buying-australian-government/ethics-and-probity-procurement> [accessed 9 February 2023].